INPUT IT Intelligence Services

400 Frank W. Burr Blvd.
Teaneck, NJ 07666
Tel. (201) 801-0050
Fax (201) 801-0441

August 12, 1996

Mr. Tetsuya Yoshida
NTT Data
Card Group
Advanced Information Network Services

Via fax 011-81-3-5546-8341
Email: yoshidatt@noa.nttdata.jp

Dear Mr. Yoshida:

Thank you for your Email of August 12.

I have made the following changes to INPUT's proposal for the study, "Trends in Card-Related Network Security".

- The timing of the two sections has each been changed from 4 weeks to 3 weeks to meet your deadline. This will finish the project by the end of September, if authorization is received this week.
- I note that you value Section (2) more than Section (1). Also, you wish to have a lower price. Consequently, we have provided the option of selecting Section (2) only, for a price of $19,000

  We do not recommend this option be exercised, however, for the following reasons:

  - We believe it is important that the products/technologies that are investigated be prioritized. Otherwise, those of little practical or market importance may be assessed while others, that are in fact more important, maybe overlooked.
  - INPUT and NTT Data need to have a common framework for assessing and understanding this market. (INPUT, by the way, believes that security and fraud issues will be extremely important in the development of networked card use.)

I did not change the proposal itself by omitting card technology (e.g., password, fingerprints) from list of possible products/technologies:

- NTT Data will have the opportunity to select, after INPUT's recommendations, whichever products/technologies it believes is important.
- In addition, INPUT believes that some forms of successful security may require card-based solutions.

I hope that this letter and the attached changes address your questions. If you have any other questions or comments, we will be happy to discuss them.

Sincerely,

Thomas O'Flaherty
Vice President

Attachment

cc. INPUT KK

Revised
PROPOSAL

TRENDS IN CARD-RELATED NETWORK SECURITY

Submitted to

NTT Data

August 12, 1996

Prepared by

INPUT

Atrium at Glenpointe
400 Frank W. Burr Boulevard
Teaneck, NJ 07666

201-801-0050
Fax: 201-801-0441

TRENDS IN CARD-RELATED NETWORK SECURITY

I. OBJECTIVES

NTT Data wishes to understand the trends occurring in card-related network security.

II. SCOPE

The scope of the study is shown in the Preliminary Report Outline attached. INPUT applied its interpretation to NTT Data's Specifications of July 31, 1996 which took into account INPUT's understanding of current and expected developments in the card security market. INPUT will be happy to discuss with NTT Data modifications in its approach and deliverable.

III. METHODOLOGY AND CONDUCT OF THE WORK

The work will be performed in two sections, which are similar to those in NTT Data's Specifications:

- Section (1): Networked Card Security Requirements

  This section will identify the requirements for networked card security. This Section will show the relative needs of different requirements and will help the prioritize the work in Section (2).

- Section (2): Networked Card Security Technology

  This Section will survey 6 product/technology areas and provide an analysis of a leading vendor or technology in each area.

IV. QUALIFICATIONS

INPUT is highly qualified to conduct this study. INPUT has a great deal of recent knowledge gained in performing research and analysis for its on-going subscription programs in

- Electronic Commerce
- Global Banking (especially its work in Electronic Banking)
- The Internet

INPUT has also conducted recent custom research studies in network-based encryption products and technologies, new developments in credit cards, forecast use of Smart Cards and computer network security.

V. FEES

INPUT's professional fee for this project is $25,000. One-half of this fee ($15,000) is due and payable upon authorization. This fee includes all expenses. The remainder of the fee is due upon the submission of the report.

If NTT Data desires, Section (2) only will be performed for $19,000. One-half of this fee ($9,500) is due and payable upon authorization. This fee includes all expenses. The remainder of the fee is due upon the submission of the report.

This fee will be reduced by 10% if NTT Data also authorizes INPUT's proposal on "Value Circulation Management Systems".

This proposal will remain valid for thirty days, unless extended in writing.

VI. AUTHORIZATION

To authorize the project as specified, please sign and return one copy of this proposal, along with the initial fee. Upon acceptance by INPUT, a countersigned copy of the proposal will be returned to.

AUTHORIZED BY: NTT DATA	ACCEPTED BY: INPUT
____________________ Name	____________________ Name
____________________ Title	____________________ Title
____________________ Date	____________________ Date

Preliminary Report Outline

CARD-RELATED NETWORK SECURITY

(1) NETWORKED CARD SECURITY REQUIREMENTS

This section will identify the requirements for card security. This is necessary so that the importance of the different security technologies in Section (2) can be prioritized.

A. Networked Card Security Risk Assessment

The risk assessment will identify which technology-based risks need to be addressed.

1. Scope: Technology-based Fraud

The are three categories of threats in using cards on networks

1. Intentional, technology-based fraud

2. Intentional, non-technology fraud ("traditional" fraud, for example, a network-based merchant does not deliver the product or service paid for)

3. Unintentional technology errors (e.g., transmission or updating errors)

This report will focus solely on the first category, technology-based fraud.

- Traditional fraud can be dealt with using traditional, largely legal, means.

- Solutions for technology-based fraud will usually address technology errors as well.

2. Classes of Fraud

There are classes and subclasses of card technology-based fraud

- Identity

    - Create a fictitious identify

    - Assume the identify of another person or organization

- Value
    - Take possession of the credit, account value or card stored value of another person or organization
    - Create fictitious value (as credit, account value or stored value)

Fraudulent identity and value exist in various combinations and these combinations have different levels of risk, as shown in Exhibit 1.

Exhibit 1

CARD NETWORK FRAUD: LEVELS OF RISK

(Preliminary Assessment)

	Take possession of the credit/stored value of another person/organization	Create fictitious value
Create a fictitious identity	HIGH RISK	HIGH RISK
Assume the identity of another person/organization	HIGH RISK	MEDIUM RISK
Use own identity	LOW RISK	LOW RISK

3. Risk Assessments

INPUT's report will assess each level of risk shown in Exhibit 1 for each of the following environments:

Closed Network Environment

- Retail
- Financial (e.g., bank ATMs)

Open Network Environment

- Retail
- Public
    - Public Access Points
    - Personal Access Points (e.g., home computer)

Note: INPUT's analysis will focus primarily on consumer use of cards

B. Strengths and Weakness by Class of Card

INPUT will assess the strengths and weaknesses of the following classes of cards using the risk assessments performed above.

Current Card Generation (Magnetic Stripe)

- Credit
- Debit
- Stored Value

IC Cards: Stored Value, Limited Processing

- Multi-purpose
- Limited Purpose (e.g., transportation)

IC Cards: Stored Value, Advanced Processing

The analysis of strengths and weaknesses will include

- Technology strengths and weaknesses
- An assessment of the business/commercial impact if weaknesses are not fixed

C. Networked Card Security Requirements

INPUT will prepare a prioritized list of security requirements for the networked use of cards. This will be used to define the types of card security products and technology reported on in Section (2) below.

INPUT will submit the Section (1) analysis and report 3 weeks after project authorization.

(2) NETWORKED CARD SECURITY TECHNOLOGY

This section of the report is directly dependent on the section above. After identifying and prioritizing, card security requirements, INPUT will survey 6 product/technology areas, including an analysis of a leading vendor or technology in each area. Exhibit 2 shows examples of these product/technology areas, along with examples of applicable vendors [in brackets].

- Both product/technology areas and vendors are shown as <u>examples.</u>
- INPUT will recommend the product/technology areas and specific vendors to be analyzed one month after authorization of the project [as part of the report on Section (1)]. INPUT will provide an explanation and rationale for its selections. NTT Data may modify these lists -- either the product/technology areas and/or the vendors to be analyzed

Exhibit 2

EXAMPLES OF PRODUCT/TECHNOLOGY AREAS

(Vendor Examples in Brackets]

- Digital certificate providers [VeriSign]
- Third party authentication [GTE]
- Encryption co-processors [Atalla]
- Security tokens [V-ONE]
- Biometric identification [Printscan]
- Magnetic stripe switches [Cardlogix]
- Card transaction standards [Secure Electronic Transaction]
- Smart card terminals [Philips]
- Fraudulent transaction identification software [Visa]
- Secure communications links [Netscape; DEC]

Note: In the RFP, card security technology was divided into the categories of

- Server systems and
- Peer-to-peer systems.

INPUT will apply these categories to the extent possible. However, products and technologies will not always fit neatly into these (or other) categories. INPUT reserves the right to introduce alternate methods of categorization.

INPUT will submit the analysis and report for Section (2) 3 weeks after NTT Data has agreed to the product/technology areas and vendors to be analyzed.

INPUT

IT Intelligence Services

400 Frank W. Burr Blvd.
Teaneck, NJ 07666
Tel. (201) 801-0050
Fax (201) 801-0441

August 9, 1996

Mr. Tetsuya Yoshida
NTT Data
Card Group
Advanced Information Network Services

Via fax 011-81-3-5546-8341
Email: yoshidatt@noa.nttdata.jp

Dear Mr. Yoshida:

Attached is INPUT's proposal and draft report outline for the study, "Trends in Card-Related Network Security".

We have modified your specifications somewhat, based on our knowledge of developments in this area. We will be very happy to discuss the Scope of the study and the report outline with you further.

As noted in our proposal, we have a significant amount of experience in this area and look forward to assisting you on this important task.

Sincerely,

Thomas O'Flaherty
Vice President

Attachment

cc. INPUT KK

PROPOSAL

TRENDS IN CARD-RELATED NETWORK SECURITY

Submitted to

NTT Data

August 9, 1996

Prepared by

INPUT

Atrium at Glenpointe
400 Frank W. Burr Boulevard
Teaneck, NJ 07666

201-801-0050
Fax: 201-801-0441

TRENDS IN CARD-RELATED NETWORK SECURITY

I. OBJECTIVES

NTT Data wishes to understand the trends occurring in card-related network security.

II. SCOPE

The scope of the study is shown in the Preliminary Report Outline attached. INPUT applied its interpretation to NTT Data's Specifications of July 31, 1996 which took into account INPUT's understanding of current and expected developments in the card security market. INPUT will be happy to discuss with NTT Data modifications in its approach and deliverable.

III. METHODOLOGY AND CONDUCT OF THE WORK

The work will be performed in two sections, which are similar to those in NTT Data's Specifications:

- Section (1): Networked Card Security Requirements

  This section will identify the requirements for networked card security. This Section will show the relative needs of different requirements and will help the prioritize the work in Section (2).

- Section (2): Networked Card Security Technology

  This Section will survey 6 product/technology areas and provide an analysis of a leading vendor or technology in each area.

IV. QUALIFICATIONS

INPUT is highly qualified to conduct this study. INPUT has a great deal of recent knowledge gained in performing research and analysis for its on-going subscription programs in

- Electronic Commerce
- Global Banking (especially its work in Electronic Banking)
- The Internet

INPUT has also conducted recent custom research studies in network-based encryption products and technologies, new developments in credit cards, forecast use of Smart Cards and computer network security.

V. FEES

INPUT's professional fee for this project is $25,000. One-half of this fee ($15,000) is due and payable upon authorization. This fee includes all expenses. The remainder of the fee is due upon the submission of the report.

This fee will be reduced by 10% if NTT Data also authorizes INPUT's proposal on "Value Circulation Management Systems".

This proposal will remain valid for thirty days, unless extended in writing.

VI. AUTHORIZATION

To authorize the project as specified, please sign and return one copy of this proposal, along with the initial fee. Upon acceptance by INPUT, a countersigned copy of the proposal will be returned to.

AUTHORIZED BY:
NTT DATA

____
Name

____
Title

____
Date

ACCEPTED BY:
INPUT

____
Name

____
Title

____
Date

Preliminary Report Outline

CARD-RELATED NETWORK SECURITY

(1) NETWORKED CARD SECURITY REQUIREMENTS

This section will identify the requirements for card security. This is necessary so that the importance of the different security technologies in Section (2) can be prioritized.

A. Networked Card Security Risk Assessment

The risk assessment will identify which technology-based risks need to be addressed.

1. Scope: Technology-based Fraud

The are three categories of threats in using cards on networks

1. Intentional, technology-based fraud
2. Intentional, non-technology fraud ("traditional" fraud, for example, a network-based merchant does not deliver the product or service paid for)
3. Unintentional technology errors (e.g., transmission or updating errors)

This report will focus solely on the first category, technology-based fraud.

- Traditional fraud can be dealt with using traditional, largely legal, means.
- Solutions for technology-based fraud will usually address technology errors as well.

2. Classes of Fraud

There are classes and subclasses of card technology-based fraud

- Identity
    - Create a fictitious identify
    - Assume the identify of another person or organization

- Value
    - Take possession of the credit, account value or card stored value of another person or organization
    - Create fictitious value (as credit, account value or stored value)

Fraudulent identity and value exist in various combinations and these combinations have different levels of risk, as shown in Exhibit 1.

Exhibit 1

CARD NETWORK FRAUD: LEVELS OF RISK

(Preliminary Assessment)

	Take possession of the credit/stored value of another person/organization	Create fictitious value
Create a fictitious identity	HIGH RISK	HIGH RISK
Assume the identity of another person/organization	HIGH RISK	MEDIUM RISK
Use own identity	LOW RISK	LOW RISK

3. Risk Assessments

INPUT's report will assess each level of risk shown in Exhibit 1 for each of the following environments:

Closed Network Environment

- Retail
- Financial (e.g., bank ATMs)

Open Network Environment

- Retail
- Public
    - Public Access Points
    - Personal Access Points (e.g., home computer)

Note: INPUT's analysis will focus primarily on consumer use of cards

B. Strengths and Weakness by Class of Card

INPUT will assess the strengths and weaknesses of the following classes of cards using the risk assessments performed above.

Current Card Generation (Magnetic Stripe)

- Credit
- Debit
- Stored Value

IC Cards: Stored Value, Limited Processing

- Multi-purpose
- Limited Purpose (e.g., transportation)

IC Cards: Stored Value, Advanced Processing

The analysis of strengths and weaknesses will include

- Technology strengths and weaknesses
- An assessment of the business/commercial impact if weaknesses are not fixed

C. Networked Card Security Requirements

INPUT will prepare a prioritized list of security requirements for the networked use of cards. This will be used to define the types of card security products and technology reported on in Section (2) below.

INPUT will submit the Section (1) analysis and report one month after project authorization.

(2) NETWORKED CARD SECURITY TECHNOLOGY

This section of the report is directly dependent on the section above. After identifying and prioritizing, card security requirements, INPUT will survey 6 product/technology areas, including an analysis of a leading vendor or technology in each area. Exhibit 2 shows examples of these product/technology areas, along with examples of applicable vendors [in brackets].

- Both product/technology areas and vendors are shown as <u>examples.</u>

- INPUT will recommend the product/technology areas and specific vendors to be analyzed one month after authorization of the project [as part of the report on Section (1)]. INPUT will provide an explanation and rationale for its selections. NTT Data may modify these lists -- either the product/technology areas and/or the vendors to be analyzed

Exhibit 2

EXAMPLES OF PRODUCT/TECHNOLOGY AREAS

(Vendor Examples in Brackets]

- Digital certificate providers [VeriSign]

- Third party authentication [GTE]

- Encryption co-processors [Atalla]

- Security tokens [V-ONE]

- Biometric identification [Printscan]

- Magnetic stripe switches [Cardlogix]

- Card transaction standards [Secure Electronic Transaction]

- Smart card terminals [Philips]

- Fraudulent transaction identification software [Visa]

- Secure communications links [Netscape; DEC]

Note: In the RFP, card security technology was divided into the categories of

- Server systems and
- Peer-to-peer systems.

INPUT will apply these categories to the extent possible. However, products and technologies will not always fit neatly into these (or other) categories. INPUT reserves the right to introduce alternate methods of categorization.

INPUT will submit the analysis and report for Section (2) one month after NTT Data has agreed to the product/technology areas and vendors to be analyzed.

INPUT®

400 Frank W. Burr Blvd.
Teaneck, NJ 07666
Tel. (201) 801-0050
Fax (201) 801-0441

FAX TRANSMITTAL FORM

Date: 10/8/96

Confidential: Y / N
Urgent: Y / N

To: Name: Renee

Tel./Location:

Co.: INPUT

Page: 1 of 3

Fax No:

File: Chron
Contact
Other:

From: Name: Janine

Subject: Rich Peterson Timesheet

Renee,
I mailed the original invoice on? last week sometime. Anyway, here is the timesheet that goes with it. I forgot to fax this sooner - Sorry!

JC.

INPUT®

Temporary Services
Task Performance Sheet

PAGE ____ OF ____ 10/4/96 Rich Peterson 10/8/96

WEEK ENDING NAME SIGNATURE DATE

SUPERVISOR'S APPROVAL ____ DATE ____

I.D. NUMBER	ORGANIZATION	HOURS ACCOMPLISHED	ACCOUNTING ONLY				ENTERED BY	
		.	.	.	.			

LABOR CODE	DEPT/PROG./ PROJ. CODE	TOTAL	Equiv. Sr. Hrs. Accomp.	#	TASK(S) (Number and type of task — see exhibit A)
	YNNT5	.	.	1	Report completed to client
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		
		.	.		

IMPACT Research, Inc.
INFORMATION SERVICES CONSULTING

RICHARD L. PETERSON, Ph.D.
President

September 26, 1996

Mr. Thomas O'Flaherty, Vice President
INPUT
Atrium at Glenpointe
400 Frank W. Burr Boulevard
Teaneck, NJ 07666

***** INVOICE *****

Current Billings:

Professional Fee:	
Networked Card Security	$12,000
Expenses:	Included
Travel/Entertainment	
Miscellaneous (Telephone)	
Total	

Total Due: **$12,000.00**

Thank you!

Federal ID: 22-2878-130

ok
Oct 2 1996
YNMT

Note: Accounts are payable upon presentation of bill. After 30 days, overdue accounts bear interest of 1.5% per month, 18% per year.

PC WORLD

PC World August 1996 v14 n8 p136(7)

Best Web browser.

(includes related article on browsers other than Netscape Navigator and Microsoft Internet Explorer, where to get browsers) (Internet Survival Guide)

Abstract

Netscape Communications' Navigator Web browser currently enjoys an overwhelming market share, and Microsoft's Internet Explorer has emerged as its only serious competitor. Navigator and Internet Explorer are the best browsers for viewing sophisticated Web content because both companies have developed their own extensions to HTML. Both browsers rate very good in ease of use, and switching between the two is easy because the interfaces are similar. Both also offer excellent performance. The two programs can both download files from one site while browsing another and handle graphics bottlenecks by offering a text-only option. Navigator is the better of the two at reading Web pages; it supports Java and plug-ins, features that have not yet appeared in Internet Explorer. Internet Explorer has better workgroup tools than Navigator, especially in version 3.0. Navigator has the edge in security, patching more holes quickly. Both programs have very good integrated E-mail and Usenet tools.

Full Text

A browser is your passport to sites and sounds on the Web. Is it time to trade in Netscape,s Navigator for Microsoft,s Internet Explorer?

Hitting a new Web site these days can be an interactive adventure. Will an animated logo or the thump of jungle drums greet you? Will you be able to stroll through a trade show held in a virtual building, or see content tailored just for you? You can enjoy all the World Wide Web's latest bells and whistles if you have the right browser--one that can take advantage of whatever a site has to offer.

Not long ago, almost a dozen browsers vied for the chance to take you to the hundreds of thousands of sites that make up the Web. But after a year of product shake-outs and some fast moves on Microsoft's part, Netscape's Navigator and Microsoft's Internet Explorer have emerged on top. Why? Both companies have blazed new trails in developing and supporting extensions to HyperText Markup Language, the programming language used to create Web pages. As a result, Navigator and Internet Explorer are the best browsers around for seeing and interacting with all the hottest Web content--from a silly slide show of Hillary Clinton's mutating hair to applications that calculate a mortgage payment. Other browsers just can't keep up. They don't support the latest HTML extensions, they're slower at downloading, or they lack features in some other crucial area. (For an update on these browsers, including NCSA Mosaic, the one that started it all, see "Where Have All the Browsers Gone?")

In this head-to-head review of Navigator and Internet Explorer, we compare ease of use, performance, Web savvy, security features, and workgroup and Internet tools. (Note: International Data Group, PC World's parent company, is a minority shareholder in Netscape Communications.) Ordinarily, we review only shipping versions of products. But Web browsers are moving targets: If you don't mind the rough edges, you can begin using beta and even alpha versions of browsers by downloading them. So for this article, we bent our rules a little and looked at the betas of Navigator 3.0 and Internet Explorer 3.0, which we pulled off the two companies' Web sites. At press time, neither beta had everything the companies had promised. So we have to reserve judgment on some features, such as Internet Explorer's support for Java. But by the

time you read this, both Navigator 3.0 and Internet Explorer 3.0 should be available in final form.

Navigator and Internet Explorer are alike in many ways. Both offer a core set of features that conform to the HTML 3.0 standard, so you can use either product to see basic Web text, headlines, images, lists, tables, and hot links. To handle the wide variety of file types that many sites now incorporate, both browsers use helper applications to display or play back data. Both have attractive, easy-to-use interfaces for easy return to favorite Web sites. Both are simple to install and a snap to acquire. Internet Explorer is free and comes with Windows 95; Navigator costs only $49.

But beyond these shared characteristics, the two browsers are waging a war of enhancements, proprietary extensions, and me-too compatibility not likely to end soon. Navigator 2.0 fired the first salvo when it added support for three Important Web tools: frames, plug-ins, and the Java programming language. Frames make Web sites easier to navigate by dividing them into multiple, independently scrollable panes. Plug-ins, third-party program modules that extend a browser's capabilities, and Java, which is used to create embedded Web apps, both make sites more interactive. Thanks to these extras, Navigator has grabbed an extraordinary 75 percent of the browser market, compared to about 10 percent for Internet Explorer.

But now it looks as if it's Netscape's turn to play catch-up. Not only can Microsoft's Internet Explorer 3.0 view frames, but the company has also developed ways to improve that technology. The beta we saw didn't have Java or plug-in support, but we expect the final version of Internet Explorer 3.0 to have those features, too. The surprise Is that Internet Explorer has become the better choice for workgroups. We tried the whiteboard, chat, and Internet phone tools that both products have added, and Internet Explorer really wowed us. Neither browser allowed more than two people to simultaneously use the phone, but Internet Explorer easily beat Navigator's one-to-one chat and whiteboard utilities by letting several people participate at once. The real tie-breaker is Internet Explorer's new application sharing capability. Using NetMeeting, you can give others control over an application or folder on your local hard drive. This feature alone could make Internet Explorer a popular way of providing technical support over an intranet, for example.

So whlch browser is better? It's a tough call. For Web surfing, either is fine. But if the idea of using a browser to work with other people appeals to you, Internet Explorer's NetMeeting is a killer set of apps.

Which browser will win in the long run? That's even harder to predict. Navigator has the popular vote, and it still does some things better than Internet Explorer, such as the way it handles bookmarks. But Internet Explorer clearly poses a serious challenge. Microsoft is giving it away--using Netscape's old tactic for accelerating acceptance. And Internet Explorer 3.0 will be able to use Navigator bookmarks, a nice bit of compatibility that Netscape hasn't bothered to provide yet. However, the biggest blow most certainly would be Microsoft's plan to make Internet Explorer the hub interface for Windows, an add-on option rumored to be available in a few months.

For a blow-by-blow comparison of Navigator 3.0 and Internet Explorer 3.0, read on. May the best browser win.

Ease of Use

Internet Explorer:Very good

Navigator:Very good

With the existence of over 7 million Web sites, you can easily drown in the Internet. Navigation shortcuts

and bookmarks help you swim safely through that flood of information. Internet Explorer and Navigator both provide bookmarks (which Explorer calls Favorites) and lots of other ways to get to sites quickly.

Both browsers cache pages you've visited so that the sites reappear quickly the next time you return to them. Both also keep a separate history of where you've been on the Web. But Internet Explorer's implementation is better. Unlike Navigator, which deletes its list of sites every time you exit, Internet Explorer maintains a history from session to session if you like, saving the URLs as Windows 95 Shortcuts.

When you find a site you want to revisit, both browsers let you mark its page and easily return to it by selecting from a drop-down list on the toolbar. But Navigator stores them in a regular HTML file, making it possible to incorporate them as hot links into your own Web pages, for example. You can easily reorder the bookmarks by dragging and dropping, and use menu options to create cascading folders. You can even create aliases for URLs, so you can insert the same bookmark into more than one folder.

Internet Explorer turns to Win 95's Shortcuts to store Favorites. You can organize your Favorites easily into hierarchical folders, just as you would any other files on your hard disk. But Internet Explorer lacks Navigator's elegant touches, like the ability to group related sites in the Bookmarks menu by drawing separator lines between entries.

What happens when your list of bookmarks gets out of date? Navigator's What's New menu option logs on to each site in your bookmark list to check whether the site content has changed. For instance, if you wanted to know every time PC World Online posted a new issue, you could check your list in Navigator instead of repeatedly accessing the site. Internet Explorer 3.0 has a similar feature in the works, but it wasn't available for testing by our deadline.

What if you head for a new site? Navigator 3.0 has the edge: It accepts abbreviated Net addresses, without the http://www. prefix and .com suffix. Internet Explorer assumes only the http:// prefix.

If Microsoft consistently does one thing right, it's help systems. Internet Explorer's help, a nice utility with an extensive Index and clear tutorials, is built into the browser. Navigator, by contrast, sends you to Netscape's Web site for help. We much prefer help files on our hard disk; after all, what use is help on a Web site if you need assistance getting connected in the first place?

Performance

Internet Explorer:Excellent

Navigator:Excellent

What's the most frequent complaint about Internet surfing? It's s-l-o-w. Your Web browser should speed things up. When it comes to bringing up sites quickly, Navigator and Internet Explorer run neck and neck.

To compare pure display speeds, the PC World Test Center measured the time that each browser needed to load several Web pages laced with performance-dragging multimedia elements. We used a closed two-PC network to eliminate any delays due to network traffic. We tested only the 2.0 versions of the browsers to avoid punishing unstable prerelease products. Navigator 2.0 and Internet Explorer 2.0 finished the renderings in a dead heat, with Internet Explorer just slightly faster.

In addition to their raw performance, both Internet Explorer and Navigator are chock-full of tricks that make your surfing speedier. Both browsers allow you to do multiple tasks at a time, such as browsing one Web

page while downloading a file from another, or simultaneously viewing two sites in different windows.

In addition, these browsers circumvent the most common downloading bottleneck--graphics--by giving you the choice to view only the text of a Web page, or to load text before graphics. In the latter case, you can often drill down into a Web site by clicking on hot-linked text, without having to wait for the graphic to appear. If you do want to see graphics, both browsers support progressive rendering, a method of speeding up a download by displaying interlaced images in several passes with increasing resolution. Progressive rendering often lets you recognize an image before it's fully drawn, so you can decide whether to stay on that page or continue on your way. Reading Web Pages

Internet Explorer:Good

Navigator:Very good

Can Internet Explorer 3.0 and Navigator 3.0 see everything on the Web? The answer is a qualified yes. Each company pushes its own HTML extensions; sometimes one browser ignores its rival's proprietary extensions or implements them differently.

For example, Navigator 3.0 supports Microsoft's Web page tags for background music and background colors for individual table cells. But it still can't display Microsoft's marquee tags. This means that if you use Navigator to view Microsoft's Web site (http://www.microsoft.com), you won't see the scrolling text that displays in Internet Explorer.

For the majority of sites, however, you won't notice any differences between the two browsers' display capabilities. Internet Explorer 3.0 can see frames and adds a couple of enhancements: New Microsoft HTML extensions will let Web sites display frames without borders, giving the page a less cluttered look. And authors of Web sites will also be able to give viewers the option of moving frames around and even minimizing some frames for convenience. Navigator, which introduced frames, corrects a sore point of its own in version 3.0. Previously, pressing the Back button took users to a previous site, not the previous frame. That snag has been fixed.

At press time we had not yet seen Internet Explorer 3.0's much-anticipated support for Java applications or Navigator plug-ins. But Microsoft promises that version 3.0 will work with both by the time it comes out in its final form, using the company's new ActiveX technology. Navigator 3.0, in turn, will use an Ncompass add-on (also called ActiveX) to read plug-ins and applications that were created with Microsoft's ActiveX.

Internet Explorer 3.0 and Navigator 3.0 will both be capable of playing video and sound files embedded in a Web page, without needing helper applications: You'll be able to hear and see what a site has to offer without having to first load an extra program. And both browsers will let you view 3-D Web sites created with the Virtual Reality Markup Language.

Have you ever linked to a foreign-language site, only to see gibberish? Both Internet Explorer 3.0 and Navigator 3.0 will provide foreign character sets so you can see these sites in their native languages. The character sets will be built in to Internet Explorer, and Navigator will use the Internet with an Accent add-on.

Workgroup Tools

Internet Explorer:Very good

Navigator:Good

Have you ever thought of a browser as a workgroup application? That's what the 3.0 versions of Internet Explorer and Navigator have become by adding whiteboards and Internet phones.

Both browsers let you and remote coworkers view the same images, annotate them, and save them to local hard drives while discussing them--all over the Internet. But Microsoft's new NetMeeting technology is more sophisticated than CoolTalk, the whiteboard and telephony bundle that Netscape acquired when it bought InSoft Inc. For one thing, NetMeeting's whiteboard and chat utilities support multiple simultaneous users, unlike CoolTalk, which allows only two people to connect at the same time.

What's more, NetMeeting lets you share your applications with other people over the Internet. We tested this feature by letting a long-distance colleague take control of a Word 7 for Windows 95 document on our local hard drive. It was slow, even with only two people connected, but it worked fine. No doubt about it: This could be the application that gives Internet Explorer the clout it needs to overtake Navigator.

Security

Internet Explorer:Very good

Navigator:Excellent

What if you sent your credit card number over the Internet and found out during the next billing cycle that somebody had siphoned off the data and used it to buy a plane ticket to Tahiti? If you're unlucky enough to fall prey to a really determined hacker, it's possible--but unlikely with either browser. Both Navigator and Internet Explorer have extensive security mechanisms built in, based on Secure Sockets Layer 3.0 and the RSA public-key encryption system. These two standards scramble the data you transmit over the Internet, preventing anyone who might be eavesdropping from understanding what you're transmitting.

Commercial Web sites that allow credit card purchases, or conduct business that involves other types of sensitive information, can take advantage of SSL 3.0 or RSA public-key encryption by applying for a certificate of authentication from an independent organization. One such organization is VeriSign (http:/www.verisign.com), a public certificate authority that provides digital authentication services and products for electronic commerce and other forms of private computer communications.

When you place an order with a certified site, its server tells your browser that the organization is legitimate. SSL 3.0 now provides personal certificates, the flip side of site certificates. A personal certificate proves that you are who you say you are (think of the certificate as a picture ID for the Internet) and prevents anyone from masquerading as you.

Downloaded Java applications can also pose security risks, according to Princeton University researchers (see Bug Watch, June). Security holes in Java and JavaScript, languages developed jointly by Netscape and Sun Microsystems, could allow programmers with malicious intent to build Java applications that tamper with your PC, say the researchers. But Netscape claims that the holes are so difficult to find that it's unlikely anyone would bother to ferret them out and use them. All the holes that the Princeton researchers identified in the programming languages have now been fixed, and Netscape will continue to patch any as they're found, said a Netscape representative. No Navigator customers have reported any problems with Java applications, he noted. According to Microsoft, Internet Explorer will help protect users from rogue applications by identifying their source and whether they've been modified since being posted.

Parental control over Web content is a growing issue. If you're concerned about your kids surfing the

seamier shoals of the Web, you'll like Internet Explorer 3.0's parental control tool, which lets you determine the levels of obscenity and violence you'll accept at Web sites. Those sites that adhere to the Recreational Software Advisory Council's rating system will be identified with a special tag, and anyone visiting an unrated or adult-oriented site will be prompted to enter a password.

Tools for Other Internet Services

Internet Explorer:Very good

Navigator:Very good

What's the Internet without interaction with others? E-mail and newsgroups are major attractions on the Net, but you wouldn't know it by looking at the anemic utilities available in Internet Explorer 2.0. But all that's changed in version 3.0: Its newsreader and e-mail clients not only now stand toe-to-toe with Navigator's, they can also be used as stand-alone products or integrated into the Windows 95 Explorer--a nice touch. Both Internet Explorer's and Navigator's e-mail utilities include address books and support for MIME, the common way to transmit binary files such as images and executable programs. The only features Navigator has that Internet Explorer lacks are address grouping and scheduled mail retrievals.

Newsgroups are another popular Internet service. Navigator's well-organized, multi-paned newsreader lets you quickly zero in on new messages. Internet Explorer 2.0 was afflicted with a dismal single-frame newsreader, but version 3.0 offers a newsreader that's very similar to Navigator's. Our beta of Internet News did not include offline reading, but Microsoft promised that the final version would.

File Transfer Protocol support? Forget it. Both browsers let you download files from the Web address line, but for uploading you should rely on a third-party FTP client such as WS-FTP32.

So which Web browser will you be having today? Netscape's Navigator 3.0, Microsoft's Internet Explorer 3.0, or both? You can't go wrong with either of these browsers. And if you really need a workgroup intranet tool that integrates with Windows 95, then look no further: For now, the winner is Internet Explorer 3.0.

Related article: Where Have All the Browsers Gone?

At one time, Netscape's Navigator was just another Web browser, with plenty of competition from products developed by organizations ranging from online services to universities. Then Microsoft rushed its Internet Explorer into the fray, and the two browsers promptly squeezed out the little guys.

We reviewed nine Web browsers besides Navigator in our June 1995 issue; here's what's happening with them today.

Cello 1.01a: There's no sign of the promised 2.0 upgrade, but the Legal Information Institute at Cornell University Law School still offers version 1.01a free from its Internet site. This browser was looking old when we reviewed it last year; by now it's positively ancient, with no support for frames or Java applets. http://www.law.cornell.edu/cello/cellotop.html

Spyglass Mosaic 2.11: Formerly Enhanced Mosaic 2.0, this browser is highly competitive with the Netscape and Microsoft offerings. You can't buy it directly, however; Spyglass sells it only to other companies for use in their Internet products. http://www.spyglass.com/products/mosaic_download.html

Internet Chameleon 4.5 for Windows 95 and Windows 3.1: Access to Web sites is only a small part of

NetManage's Internet Chameleon 4.5. This package's selling points are its dial-up ability and integration among 18 different Internet utilities. Its Web browser, on the other hand, is relatively weak. http://www.netmanage.com/netmanage/products/intcham.index.html

InternetWorks 1.0 Internet: Works is now bundled with America Online's Global Network Navigator service and isn't sold commercially. http://gnn-e2a.gnn.com/gnn/join/joingnn/member.html

Mosaic in a Box for Windows 95: CompuServe Internet Division (formerly known as Spry) released Mosaic in a Box for Windows 95 last August. The browser hasn't kept up with the times, however. It lacks support for leading-edge elements like frames and HTML tables. http://support.spry.com/public/mbox/

NCSA Mosaic 2.1.1: The National Center for Supercomputing Applications deliberately waits until new features are widely accepted standards before integrating them into NCSA Mosaic, now at version 2.1.1. NCSA Mosaic handles the majority of Web sites without a problem, but look to Navigator or Internet Explorer for viewing the spots that use the hottest design techniques. http://www.ncsa.uiuc.edu/SDG/Software/WinMosaic/

NetCruiser 2.1: Netcom's NetCruiser 2.1 is available only with a Netcom account. http://www.netcom.com/netcom/netcrz.html

SuperHighway Access 2: SuperHighway Access 2 packs nearly as many features as Internet Explorer or Navigator. But some of the problems we complained about back in our June 1995 review are still around. (For example, you still can't cache documents from previous sessions.) http://www.frontiertech.com/products/sha2.htm

winWeb 1.0 A2.3: winWeb no longer exists as a stand-alone product. EINet, now TradeWave, incorporated the browser into Virtual Private Internet 2.0, a tool kit to build secure corporate intranets. http://galaxy.tradewave.com/tradewave/products/tradevpi.html

--Amy Helen Johnson

Related article: Where to Get Them

How can you get a copy of Navigator or Internet Explorer? Let us count the ways. Like a couple of politicians in an election year, Netscape and Microsoft are campaigning hard to win you over to their camp. Following is a quick guide to picking up one (or both) of the most popular Web browsers.

Web sites: Nothing beats free, which is what Internet Explorer is--at least for now. Not only does it come with the Windows 95 operating system, but you can also download it at no cost from Microsoft's Web site (http://www.microsoft.com). You can download a copy of Navigator from Netscape's site (http://home.netscape.com), but it's no longer free. By the end of the 90-day evaluation period, you'll need to ante up $49.

Online services: Thinking of subscribing to an online service? CompuServe and America Online will soon make Internet Explorer their default browser, with Navigator as an option. Prodigy will offer Navigator, but not Internet Explorer.

ISPs: If you decide to access the Internet through an Internet service provider, you're likely to wind up using either Navigator or Internet Explorer as your Net interface. Literally hundreds of service providers, ranging from AT&T to small start-ups such as Earthlink, bundle or recommend one browser or the other. Microsoft

holds the edge in sheer number of deals struck, probably because it provides Internet Explorer to service providers at no cost.

Off the shelf: Both browsers are available retail or from the vendors in special packages. Navigator Personal Edition (which also sells for $49) adds a dial-up kit. (You can use Microsoft's dialer with Internet Explorer if you have Windows 95.)

Microsoft's $10 Internet Starter Kit bundles Internet Explorer with step-by-step instructions for beginners and 30 free hours on the Internet via The Microsoft Network.

--Carla Thornton

Type

Software Review
Evaluation

Company

Netscape Communications Corp.
Microsoft Corp.

Product

Microsoft Internet Explorer 3.0 (Web browser)
Netscape Navigator 3.0 (Web browser)

Topic

Web Browser
Software Multiproduct Review

Record #

18 512 922

PC Magazine April 23, 1996 v15 n8 pNE36(1)

Spry SafetyWeb Server.

(one of three evaluations of Windows NT-based Web servers in "The Web Rolls On") (Network Edition: First Looks)

Author

Tabibian, O. Ryan

Abstract

The $1,295 SafetyWeb Server from Spry's CompuServe Internet Div is an easy-to-use package with built-in security and database connectivity at an affordable price. One of the most useful features is its set of ODBC drivers that allow users to easily link SafetyWeb with best-selling databases. The server includes a number of other excellent features, including multihosting, a suite of desktop tools and Secure Sockets Layer security. One of its best features is its Proxy Server, which allows users to beef up security by providing one point of entry and exit on the network. SafetyWeb is impressive in terms of ease of management and functionality. On the downside, it does not allow users to import user databases from Windows NT. Instead, users must manually create users. A free version, called Spry Web Server, is available on the Web, but it lacks some of the features found in SafetyWeb.

Full Text

Since the beginning of the Internet revolution, Spry has been known for providing desktop tools for connecting to the Internet. Now the next step has been taken. The company, recently acquired by CompuServe, has finally released its long-promised Web server--Spry SafetyWeb Server. It lives up to much of its prerelease hype by offering an easy-to-use server with built-in database connectivity and security at a reasonable price.

We tested the Microsoft Windows NT version of SafetyWeb Server ($1,295). It also comes in BSDIA, HP-UX, SGI IRIX, and Solaris 2.4 variants. SafetyWeb Server has the distinction of being one of the few non-Microsoft products to carry the Microsoft BackOffice Seal.

One of the product's most useful features is its included set of ODBC drivers. These let you easily link the server with popular databases like Microsoft Access. And prepackaging the drivers eliminates the need for complicated Common Gateway Interface (CGI) scripts to add database connectivity to Web sites.

SafetyWeb has other excellent features as well: Secure Sockets Layer (SSL) security, multihosting for setting up multiple Web servers with different IP addresses on the same server, a proxy server, and Internet Office Pro, a suite of desktop tools.

The package also includes Architext Software's Excite search engine and SoftQuad's HoTMetal PRO HTML editor. With Excite you can quickly create search engines for your Web site, and HoTMetal lets you create Web pages without manually adding HTML tags. HoTMetal is limited, however. Really best for novice users, it doesn't support some of the advanced HTML options, such as varying font sizes and scrolling text.

We installed the SafetyWeb Server on a Windows NT 3.51 Server and found the process simple and straightforward. Basic installation and configuration took only a few minutes, but configuring the security portion of the server was more complicated. Like Commerce Builder, it required a digital certificate from a certification authority.

Once installed, the server impressed us with both its functionality and ease of management. With the graphical management utility, you can centrally manage all aspects of the server, including setting up security, creating multiple servers, and setting port numbers from a single console.

Also, the server was well integrated with features within Windows NT. For example, you can add Web-server statistics to the Windows NT Performance Monitor and view critical Web-server information, such as total transactions and maximum concurrent sessions.

You can also manage SafetyWeb remotely from any Windows NT or Windows 95 machine on the network. But unlike Netscape Commerce Server, you can't manage SafetyWeb from anywhere on the Internet.

SafetyWeb does not take advantage of the Windows NT user database. It requires you to create users manually instead of importing them from the Windows NT database as you can with Commerce Builder.

One of SafetyWeb's best features is Proxy Server, which lets you tighten security by providing a single point of entry and exit for your network. SafetyWeb, however, cannot create URL filters that deny internal users from accessing certain sites.

Several logging options come with SafetyWeb. You can create a log file in either the Common Log format or the more recently released Combined Log Format, which can gather more critical data.

With Combined Log Format, you can collect information such as referrer, the URL of the server that the visitor comes from, and browser, the type of browser and operating system the visitor is using. Thanks to the ODBC drivers, you can import any of these logs directly to a database for easy manipulation and reporting.

Spry Web Server, a free version of this product, can be downloaded from the Web. The freebie, however, doesn't include SSL, Excite, HoTMetal, or Internet Office Pro.

Spry SafetyWeb Server 1.0. List price: $1,295. Spry, CompuServe Internet Division, Bellevue, WA; 800-447-2971; fax, 206-557-6000;

Type

Software Review
Evaluation

Company

Spry Inc.

Product

Spry SafetyWeb Server (Internet/Web server software)

Topic

Internet/Web Server Software
Software Single Product Review

Record #
18 205 056

Computer Letter

Computer Letter July 15, 1996 v12 n23 p8(1)

At random; how many keys do you have?

(PGP, Viacrypt merge) (Company Business and Marketing)(Brief Article)

Full Text

With the merger a week ago of PGP and Viacrypt, it looks like we'll be seeing a rather interesting experiment in consumer software: the first serious test of the market for personal privacy. PGP, which was formed recently by Phil Zimmerman, inventor of the freeware encryption program called Pretty Good Privacy, will get Viacrypt's customer base of 10,000 or so users of the commercial-grade version of PGP, which Viacrypt licensed from Zimmerman a couple of years ago. To date, Viacrypt has been selling PGP mostly to business users through direct sales, primarily for e-mail encryption. With the merger, however, Zimmerman and Tom Steding, who will be CEO of the new company, hope to expand the potential user base to some 2.5 million by pushing PGP through retail outlets for the first time.

Viacrypt's success to date is certainly encouraging; sales are doubling every six months. Will the average consumer find a use for personal encryption? Given the fact that many business e-mail users are increasingly telecommuters, plus the fact that e-mail is for some becoming an important part of their lifestyle, it's quite possible that Mr. Steding and Mr. Zimmerman could get a boost just from selling into the installed base of corporate e-mail customers. If it works out, PGP could jump-start an entire industry of consumer security products. Mr. Zimmerman already has a freeware product that encrypts Internet phone conversations, but additional packages could be offered for, say, providing encryption for Web documents on top of the Secure Sockets Layer technology used by many Web servers. Who knows? Web shoppers, armed with their own security keys, might even feel a little safer about spending that e-cash.

Company

PGP
Viacrypt

Topic

Company Acquisition/Merger

Record #

18 500 666

CommunicationsWeek

CommunicationsWeek July 8, 1996 n618 p1(2)

Oracle signs with RSA for digital signature.

(RSA Data Security Inc) (Company Business and Marketing)

Author

Marshall, Martin

Abstract

Oracle Corp has signed an agreement with RSA Data Security Inc that will change how the software vendor approaches its encryption strategy. Oracle's shift to an overall encryption committment instead of a product-by-product approach will be effected by integrating RSA Data Security technology into the company's enterprise workflow programs. Users will also be able to access non-Oracle applications and network resources with a single login and digital signature. The move to provide an overall data security strategy is prompted by threats to data integrity on the Internet. Many companies are currently holding off on Internet plans until their security fears can be allayed. RSA Data Security technology will first surface in Oracle's Advanced Networking Option, which is expected in fall 1996.

Full Text

Oracle next week will disclose a sweeping change to its data security strategy. The company will shift from a case-by-case approach to an overall commitment to encryption technology from RSA Data Security Inc.

RSA's digital signature technology will be integrated into Oracle's enterprise workflow applications, putting in place the safeguards needed to extend these applications to the Web. It also will allow users to access non-Oracle applications and corporate network resources by using a single login with a digital signature.

The agreement between RSA, Redwood City, Calif., and Oracle addresses the most common corporate fear regarding the use of the Internet to access corporate applications and services-the perceived threat to data integrity. Oracle's RSA technology may help a number of companies take the Internet plunge.

"We're looking at Internet deployments to tie in our customers as well as third parties that sell and service our products. But security is clearly a prime issue for us because we have a great deal of sensitive data," said James Bosco, project manager at Hartford Insurance, Simsbury, Conn. "Public key encryption seems to be where the market is going, and it seems to be addressing all of the issues. Anything that Oracle can do in this area will be extremely helpful."

"RSA's data-encryption scheme represents very serious authentication," agreed Ezra Gottheil, senior analyst at the Hurwitz Group Inc., Newton, Mass.

The RSA digital signature technology will first show up this fall in Oracle's Advanced Networking Option, which contains Oracle's Secure Network Services, according to Paul Lambert, director of server products for the software developer. Later, it will appear in Oracle's InterOffice products and corporate applications such as Oracle Financials.

Oracle has just begun to examine how its tools products, such as Developer 2000 and Designer 2000, can incorporate digital signatures, Lambert said.

Oracle's Web Browser, Web Server and Oracle Mobile Agents already contain some other forms of the RSA

encryption technology. Noteably, the Oracle Advanced Networking Option to SQL*Net supports RSA's RC4 encryption algorithm as well as the Data Encription Standard (DES40) and also offers the ability to implement a customized security solution. Public-key encryption technology will eventually find its way into all Oracle products, Lambert said.

Sign Me Up

The digital signature will eventually find its way into ordinary office transactions, such as managers signing off on documents in a workflow environment, or authorizing payments. To obtain a valid digital signature, individuals must register for a unique X509 certificate of authorization with a trusted third party such as VeriSign Inc., GTE Corp. or the U.S. Postal Service's Electronic Commerce Services.

The number of X509 certificates is in the tens of thousands, but that will soon jump to tens of millions, according to Kurt Stammberger, director of marketing at RSA. "The initial rollouts of X509 have been with programmers and secure servers, but soon anyone who needs to prove to a third party that a transaction has taken place will need one," he said.

Digital certificates come in multiple levels, with a more trusted commercial certificate costing about $300, but the first level of certificate, which most people will use, is available free to people who sign up via the Internet. Stammberger said that the next version of Netscape Communications' browser will include a free X509 authentication certificate.

He also notes that the deal with Oracle follows deals already in place with IBM, Microsoft, Netscape and Sun Microsystems, all of which use RSA's Bsafe cryptography engine for encryption and decryption across the Net. Microsoft has exposed a lower-level API of the digital signature in its Crypto-API tool kit, Netscape in its Secure Sockets Layer and IBM in its Generic Security System.

"The deal with Oracle is a positive one for developers both inside and outside the Oracle community," Stammberger said. "It enhances everybody's security and signals a trend that will be used through all big vendors."

How quickly corporate developers will jump on the digital-signature bandwagon may depend greatly upon whether they see it as a critical competitive advantage or disadvantage, according to Hurwitz's Gottheil.

Multiparty Transactions

Corporations have been hesitant to plunge into multiparty Internet commerce because business transactions often involve as many as six different parties, each of which may have a different corporate firewall. If even one of the firewalls involved in the transaction is different from the others, there is the possibility that the transaction could be impossible, according to Hurwitz's Rugullies.

To solve this problem, RSA brought together the six leading firewall vendors to establish an Internet Protocol Security (IPSec) specification. Last month, it completed a common implementation of IPSec, called Secure Wide Area Network (S/WAN), and tested all the firewall vendors against each other. "The results are posted on our Web site [www.rsa.com]," Stammberger said. "We're getting there."

Jeffrey Jacobs, of Jeffrey Jacobs & Associates, whose Belmont, Calif., consulting firm integrates Web-based systems for Kaiser Permanente, Nation-wide Insurance and Bristol Meyers/Squib, said that most of his clients are just beginning to think about adding security to their Web applications.

"At this stage, most of my direct customers are into Web-based publishing rather than Web-based commerce. There is security in the back-end systems, but the materials going out over the Web are informational materials, not financial ones," he said.

But according to security research analyst Erica Rugullies, also at the Hurwitz Group, the basis of corporate hesitation to deploy Internet applications has been more psychological than technical. "People are used to handing their credit cards across a retail counter, " she said, "but they don't stop to think that the risk of doing that can be even greater than putting it across a wire."

Oracle can be reached at www.oracle.com or 415-506-7000.

Company

Oracle Corp.
RSA Data Security Inc.

Topic

DBMS
Data Security Issue
Encryption
Company Licensing Agreement

Record #

18 462 334

Computer Shopper Oct 1996 v16 n10 p70(2)

Office-data encryption can be expensive but invaluable: companies strive to decipher choices amid lack of standards.

(Technology Information)(Brief Article)

Author

Tadjer, Rivka

Full Text

Joe Bierley, director for law-enforcement programs at the Torrance, Calif., system-engineering company Logicon Corp., had a problem. He needed to find a way to keep sensitive law-enforcement-agency data secure from unauthorized eyes, both internally and externally.

After several months' search, he settled on Nortel Corp.'s Entrust client/server software system. Entrust provides public-/private-key encryption technology for a price of $6,000 for the server plus $150 per seat.

"[Entrust] offers strong security services, and the environment we're working in demands that there's no acceptable lesser standard," Bierley says. "We have to protect the information we're required to protect. We did a fairly thorough evaluation of what's on the market, too. We can't use the Internet or Internet-based technologies at all for what we do--we have privacy as well as security restrictions."

For a growing number of businesses in the same boat, market-research firm International Data Corp.'s (IDC's) surveys indicate an urgent need for some sort of data-encryption solution. But IDC's research also suggests that the encryption options on the market today leave office managers feeling frustrated instead of secure.

"Encryption is definitely important now, but there's no market, really," says IDC analyst Paul Mason. "There aren't a lot of choices, and a lot of the choices that exist are either inadequate or illegal." The latter, he explains, are products that violate U.S. export laws currently limiting encryption keys to 40-bit length, even though these days 40-bit keys are relatively easy to crack. (See the sidebar, "U.S. May Loosen Encryption Limits.")

Nearly every business manager may be tempted by the concept of encrypting at least some of the data that resides on office desktops or that travels over modem, LAN, or WAN conduits. The problem for corporations today, Mason says, is finding a data-protection system that's reliable and scalable across a variety of sites and applications.

"There's a lack of standards for data in transit as well as data on the system," he says.

Still, the fact that customers like Bierley are able to find secure, albeit expensive, solutions is encouraging to onlookers like Steve Young, an electronic-commerce analyst with the Mountain View, Calif.-based market-research firm Input. Young says that not only Nortel--a business unit within Northern Telecom--but RSA Data Security, Terisa Systems, and Trusted Systems are all selling client/server products today.

"The telling market factor for the growth of the encryption market is electronic commerce," Young explains. "If you believe that Internet commerce will be big over the next five years, encryption technology will be

essential to that growth and will grow in step." He adds that even corporations such as Logicon, which have no intention of using the Internet for transporting mission-critical data, will benefit from the boom in electronic commerce, which Input estimates will grow to $255 billion by 2000.

Public-/private-key encryption remains the most popular method of securing data and verifying users' identities. (See the October 1995 Connections article, "Feeling Safe and Sound Online," p. 620.)

"Whether over the Internet, or on two separate seats on a LAN, people share keys to encrypt and decrypt [information]," Young says. "But the key question is: How do you know if I'm who I say I am?"

That's the rationale behind digital signatures--authentications of e-mail addresses and other information, issued by a certificate authority or third party with no vested interest in whether a person's identification is valid. Young likens certificate suppliers such as Verisign (http://www.verisign. com) to the Department of Motor Vehicles, which doles out driver's licenses and other IDs to the public. Other organizations planning to offer certification services to consumers and businesses range from GTE to the U.S. Postal Service.

As for potential players such as Microsoft Corp. and Netscape Communications Corp., Young thinks such companies may provide the underlying technological advances, but won't become certificate providers.

"Microsoft has the technical capability, but not the service-providing arm," he says. "People will more likely trust some company like the Postal Service because it doesn't have a vested interest."

All these market forces and psychological issues, however, could take a backseat to the perennial problem of standards. Who wants to pay hundreds of thousands of dollars when an encryption system could be rendered obsolete in a few years?

"There are no standards yet, so today, all public/private encryption systems are functioning separately," declares Shauna White, Nortel marketing manager.

The Internet Engineering Task Force (IETF) has been working to change that. In September 1995, the industry association formed the Public-Key Infrastructure subgroup to create an algorithmic solution to incompatible encryption systems, according to Paul Van Oorschot, chief of security architects at Nortel and a member of the task force. Oorschot says IETF members such as Microsoft and Netscape have been active participants, and the arrival of such a standard is imminent. He would not provide a firm date.

If companies hesitate to spend big bucks for a security system before standards arrive, Young advises, they can try relatively inexpensive software tools such as Symantec's Norton Your Eyes Only or shareware products such as Pretty Good Privacy (PGP), available for download from http://www.pgp.com.

"In terms of reliability, PGP is as secure an algorithm as any other encryption option," Young says, although it does not support client/server administration. "You may have to cobble things together, but [something like PGP] may be a good way to test encryption out," he adds.

And even if a company opts for a deluxe encryption system that later becomes obsolete, Young points out, the business will have least gotten a few good years' use out of it, or a few years' freedom from data thieves.

Topic

Encryption
Technology Overview
Software Selection

System Selection
User Need

Record #

18 709 385

PC MAGAZINE

PC Magazine Sep 24, 1996 v15 n16 p34(1)

Virtual plastic: banks to issue digital Visas.

(VeriSign to provide authentication services for Visa on the Web) (Internet/Web/Online Service Information)(Brief Article)

Author

Rupley, Sebastian

Full Text

Security concerns have held back Web-based commerce, but Visa and VeriSign are getting close to what could be widespread, secure credit-card transactions.

VeriSign is aiming to provide authentication services for Visa's "virtual" credit cards by the beginning of next year. The Visa/VeriSign system calls for VeriSign to provide digital authentication certificates based on the Secure Electronic Transactions (SET) standard, which is also backed by MasterCard, GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, and Verifone. SET calls for encoded digital certificates that people can use as the equivalent of credit cards for electronic transactions. VeriSign will provide the service on behalf of Visa, which, in turn, will make it available for Visa-accepting financial institutions.

According to Steve Herz, senior vice president of electronic commerce at Visa International, "Banks will be able to offer their cardholders and merchants 'bank-branded' certificates for conducting secure business."

In practical terms, after selecting your purchases on the Web, you'll click on a credit-card icon that's linked to your unique "decoder key." Then you'll fill out an e-mail form that includes the decoder key, a list of the items you want to purchase, and a digital certificate, and pinpoints the bank that issued the Visa card. The merchant uses the decoder key to process the order.

VeriSign's Web site will make SET test certificates available for application developers who intend to sell SET-certified products. Later this year, commercial tests will take place. And by the first quarter of 1997, Visa hopes to be issuing digital credit cards.

Company

VeriSign Inc.
Visa International

Topic

Electronic Commerce
Internet/Web Technology Application

Record #

18 651 329

PCWEEK

PC Week Sep 16, 1996 v13 n37 p1(2)

IBM boosts encryption initiative.

(Company Business and Marketing)

Author

Moeller, Michael

Abstract

IBM plans to announce SuperCrypto, an security initiative designed to simplify encryption and a key-recovery scheme that may allow developers to export encryption algorithms greater than 40 bits. SuperCrypto classifies encryption technologies as APIs, engines, services or applications. IBM will expose the APIs in its own applications and services as part of the effort. The key-recovery technique makes it easier to create and manage a recovery key that can decode data encoded with a large encryption key. IBM seeks industry support for the recovery key technique, and some believe the technology will meet the government's criteria that it be able to access encoded data on demand. The US currently prohibits exportation of any data encrypted with algorithms bigger than 40-bits, but IBM hopes that its technology will encourage the government to relax the policy, since a decryption key will be readily available.

Full Text

IBM will roll out several security initiatives next month that include a new way to build encryption into software and technology that could enable U.S. companies to export products with strong encryption algorithms.

In New York early next month, IBM is expected to announce SuperCrypto, an umbrella strategy that attempts to categorize encryption schemes into four areas: applications, services, APIs and engines, sources said.

IBM also will introduce several "key-recovery" technologies that could enable businesses to export encrypted data or software beyond the current 40-bit limit--without breaking U.S. government restrictions.

"We want to use strong encryption, but we have to worry about if we are going to break any laws in different countries and in the United States when we use a product or write our own," said John Swartzendruber, an information consultant at Eli Lilly and Co., in Indianapolis. "It has to be very easy to use if you want security to be used by end users; otherwise, it is just overlooked."

IBM's new techniques promise to simplify the generation and maintenance of a "recovery" key that unlocks data that is stored or sent using a large encryption key, such as the 64-bit Data Encryption Standard key, said sources.

IBM is attempting to garner industry support for the new key-recovery technology and is expected to license the technology to Netscape Communications Corp. and Sun Microsystems Inc., said sources.

The sources also added that the technology may satisfy the requirement imposed by the U.S. government that it be able to access encrypted data on demand.

Last year, the federal government proposed a "key escrow" concept that would have enabled corporations

and U.S. software vendors to use strong encryption schemes, as long as the government could hold onto a key to unlock the encrypted message.

This proposal was criticized by the software industry and has yet to be widely supported because of fear that key escrowing could be easily abused.

Sources believe the government may relax its encryption export policies if a business or corporation held a recovery key that could be subpoenaed by the government.

For software development, SuperCrypto is IBM's attempt to make it easier for ISVs to implement encryption technologies.

For example, IBM plans to expose the APIs within such applications as Net.Commerce and within services such as Cryptolopes, its secure World Wide Web distribution technology, sources said.

IBM is not alone in its effort to ease the use of cryptography. Microsoft Corp. last week unveiled its CryptoAPI Version 2.0 (see story, Page 19). Hewlett-Packard Co. also is working on a similar architecture called Internet Crypto Framework.

ISVs believe that these API framework efforts are just the first of many to come out in the near future.

"We believe we can be compatible with all of them," said Gary Sabo, vice president and general manager of the Internet Business Group at Atalla, of San Jose, Calif. Atalla is building a cryptographic coprocessor that can be installed as a separate box or as a PC Card.

Additional reporting by Norvin Leach

Unlocking Security: IBM's new encryption plans

* SuperCrypto, an architecture that supports smart cards, crypto chips, tokens and authentication and encryption software

* Create new key-recovery technologies

* Create a single application for exportation outside the United States

---

Company

International Business Machines Corp.

Topic

Company Technology Development
Encryption

Record #

18 691 106

Electronic News (1991)

Electronic News (1991) April 15, 1996 v42 n2112 p34(1)

Atalla, VLSI team on secure data chip.

(VLSI Technology) (Company Business and Marketing)

Author

MacLellan, Andrew

Abstract

VLSI Technology and Atalla have teamed to create a data security chip that will make electronic commerce on the Internet as secure as automatic teller machines (ATM) and point-of-sale (POS) equipment. The agreement calls for development of a single chip through three phases with the first phase involving a new generation of Atalla's WebSafe device for Web server data encryption applications. The second phase involves migration to the board level, and the final phase will involve migration to a single ARM, 32-bit RISC processor that has RC2, RC4, data encryption standard (DES) and RSA data security. Both companies will contribute heavily to research and development and will share marketing rights, though each may separately license the technology to OEMs.

Full Text

San Jose, Calif.--Atalla and VLSI Technology this week will pool their respective data encryption expertise to stimulate commerce over the Internet, promising to deliver a one-chip system which offers the end-to-end security of current point-of-sale (POS) and automatic teller machine (ATM) transactions.

The joint development effort, which also targets corporate intranets and financial service networks, will manifest itself initially in a new generation of Atalla's stand-alone WebSafe device for Web server data encryption. The technology track will then migrate to a board-level product, the companies said, culminating in 18-24 months in a one-chip, ARM 32-bit RISC processor with on-board RSA data security, data encryption standard (DES), RC2 and RC4 encryption and VLSI's proprietary one-time programmable vROM.

According to the open-ended agreement, both Atalla and VLSI will commit substantial R&D resources to the project, share marketing rights and may separately license the technology to OEMs.

"VLSI, with its technology in semiconductor silicon, is giving us the ability to put together a much higher performing product than is available on the market today," said Larry Hines, director of technical support for Atalla's Internet Products business unit. "We are providing the commercial applications, VLSI is bringing the semiconductor expertise, and we will marry the two."

Atalla, a division of Tandem Computers since 1987, has a history of encryption development, as does VLSI, which entered the market in 1991 with a DES stand-alone chip and has moved since into data encryption for cable modems, set-top boxes, PCMCIA cards and other applications. VLSI's DES chip, based on an algorithm which has been used in commercial-grade encryption applications for more than 20 years, also appeared in Atalla's earlier generation WebSafe devices.

Indeed, it was VLSI's ability to offer data encryption in a silicon package--as well as the company's write-once ROM--which attracted Atalla 18 months ago when it began looking for ways to shrink the footprint of its financial data security product line.

"With vROM we have a secure application," said Mr. Hines. "If I need to change it, I don't have to do a ROM mask, we can rewrite the program. It can be as simple as one command change."

In a market which is expected to ramp from 1995 sales of $395 million to $5.6 billion by the end of the decade, according to the Yankee Group, both Atalla and VLSI are pushing IC-based technology over software algorithms. According to Mr. Hines, a single chip, installed on the motherboard of a PC, for example, will carry out the most computationally demanding encryption functions, unlike a software algorithm which can overload the system CPU and disrupt Internet transactions. The new technology also is said to enable 200 transactions/second, as opposed to existing merchant protocols which generate only about one-and-a-half.

In addition to higher performance, products based on the Atalla/VLSI chip will cost less. Mr. Hines said an existing ATM-only POS device, which is priced at about $50,000 per system, could be replaced with a next-generation WebSafe with broader encryption features and a $12,500 price tag.

Perhaps the most important feature of the system-on-a-chip, however, is end-to-end security, a function which both companles are counting on to dispel consumer fears about engaging in financial transactions over the wire. Unlike software, which may be breached through memory dumps or a bus monitoring program, the hardware key management of the encryption chip Is more robust and offers a physical layer of protection. In fact, in addition to the fortification inherent in silicon, the new encryption device is said to include tamper-resistant features which detect temperature changes, tilt and vibrations caused by drilling or other attempts at unauthorized access.

The first market segment identified under the companies' roadmap are financial and commercial institutions which are clamoring for a secure way to send monetary transactions, Intellectual property and engage in other forms of commerce both over the Internet and internally through an intranet or other networking system. The next phase of the plan will Involve end-users interested in home banking applications, with both Atalla and VLSI planning moves onto the PC and, later, into set-top box and PDA applications.

Beta samples of the WebSafe 3 are expected out in September, with first customer shipments following in 4Q96.

Company

Atalla Corp.
VLSI Technology Inc.

Topic

Cooperative Agreement for Product Development
Electronic commerce

Record #

18 218 705

Newsbytes

Newsbytes April 2, 1996 pNEW04020021

Digital Pathways' Windows NT Security Server.

Full Text

BASINGSTOKE, ENGLAND, 1996 APR 2 (NB) -- Digital Pathways has started shipping the Defender Security Server for Windows NT (DSS NT), which it claims is the market's first security server running under the Windows NT operating system.

According to Colin Tankard, a senior spokesman for the company, DSS NT is a software application that runs on standard Intel or PowerPC processors and provides authentication services to protect access to enterprise networks through communication servers.

The Defender Security Server is the first of a suite of NT authentication and management applications to be announced by Digital Pathways that will provide a complete security solution on NT.

"We believe that the larger commercial and government organizations will standardize to a large extent on the NT platform," he said. He added that the system is at the "cutting-edge" of security systems that are based on "open" standards.

In use, DSS NT's distributed, scalable architecture permits simultaneous authentication to all access points on the network. Authentication can occur from a single or multiple Microsoft or Windows NT remote access servers, as well as communication servers such as Shiva LanRover and Microsoft Remote Access Server.

DSS NT allows users to take advantage of any wide area service, including dial-up, ISDN (integrated services digital network), X.25, GSM (global system for mobile communications), frame relay, and ATM (asynchronous transfer mode). The server provides extended user authentication through firewalls, for Telnet, FTP (file transfer protocol) and remote log-on services, and eliminates the need to install proprietary hardware at each network access point.

According to Tankard, users are authenticated through one-time passwords generated by the DSS NT and SecureNet Key tokens. DSS NT supports standards-based transport protocols, including TCP/IP Transmission Control Protocol/Internet Protocol) for LAN (local area network) transport.

The network system can also be set up for load sharing to avoid traffic overload or delays in the authentication process. As an added advantage, the primary and alternate DSS NT server can be active at the same time, which prevents delays or lack of secure remote access in the event of a system or transport failure.

The system, which starts from UKP1,900, automatically switches after a specific number of failed authentication re-tries, without having to wait for time-based switching.

(Sylvia Dennis/19960329/Press Contact: Ingeborg Seel, tel +44-181-758-2521, fax +44-181-847-1079, Internet e-mail ingeborg.seel@parabox1.parasoft.co.uk; Reader Contact: Digital Pathways, tel +44-1256-882191, fax +44-1256-882008)

Record #

18 150 175

CommunicationsWeek

CommunicationsWeek Nov 13, 1995 n584 p63(4)

Encryption+firewalls+passwords+token authentication+user ID=security overkill?

(includes related articles on vocabulary, tips, security manager) (Industry Trend or Event)

Author

Robinson, Teri

Abstract

No network can ever be entirely secure, and some companies waste thousands of dollars and network resources in over-securing their networks. Businesses should determine which information is the most important to them and then assess the realistic threats to that information. The next step is to decide which security measures will be appropriate for safeguarding the different types of information and to create a policy that governs how the network is set up. Users must them decide how much money is available for security costs. Users need to beware of simply reusing a solution that worked well in the past. Encryption protects data, but it also increases network traffic and slows response time. Many products come with built-in, easy-to-use security features that users ignore, causing them to spend more on duplicate features. Security procedures should be transparent to end users, because they will find shortcuts for cumbersome processes.

Full Text

Network managers target security as a top priority, but failure to assess risks accurately can be murder on budgets and productivity

Every network manager wants a secure network, but too much security can prove costly and counterproductive. Not every bit of data begs for encryption, not every subnetwork demands a firewall and not every user requires multiple passwords. Yet observers say companies consistently overspend on security to overprotect their assets-only to suffer security breaches anyway.

"You don't want to spend $50,000 fixing a $10,000 problem-and leave a $1 million hole," says Digital Equipment Corp. security consultant Dave Cullinane.

On the other hand, you don't want to find yourself in Citibank's predicament: Despite security precautions deemed by many observers to be among the tightest in the financial community, the bank discovered last fall that an electronic bandit had successfully bypassed the bank's security measures to make off with anywhere from $10 million to $400 million, according to estimates.

Ernst & Young, New York, estimates that one in four U.S. companies has been a victim of computer crime. Annual losses incurred from information theft range from $1 billion to $15 billion, according to LeeMah DataCom Security Corp., Hayward, Calif.

Compounding users' security fears are the latest reports of inherent security flaws in the Internet, prompting security software vendors such as Netscape Communications Corp., Mountain View, Calif., to launch extensive efforts to identify the weaknesses and redesign security programs.

Can any network ever be 100 percent secure? Probably not. Part of the problem is that there is no clear-cut set of rules for security coverage. Every company has unique security needs, which means too much security at one company might be too little for another, according to Mike Grandinetti, director of marketing

at Raptor Systems Inc., Waltham, Mass., a firewall vendor.

Some companies overprotect their networks by buying "Fort Knox security to go around a 7-Eleven," says Carl Megelich, vice president of marketing and business development at Digital Pathways Inc., Mountain View, Calif. But when does enough security become too much? Even the experts disagree.

"There are a lot of different approaches," says Bill Maguire, communications manager at Sprint United Telephone, Winter Park, Fla. "A lot of people believe you should leave security to the host, but I don't believe it." Maguire bases his strategy on a simple concept. "The primary thing is to keep intruders out of the network," he says. "Once you've done that, you don't have to worry about them using passwords."

Vendors don't offer further elucidation on the subject. Some routinely advise against installing security measures that simply assuage customer paranoia, while others, like DEC's Cullinane, believe the customer is always right.

How can you be sure you've taken the right steps to protect your corporate network adequately without going overboard?

Assess Your Risk

The first step is to assess your business risk. "You have to know where the family jewels are," says JoAnn Perry, principal of JoAnn Perry & Associates, a security consulting firm in Sparks, Nev. "The security has to match the business risk, otherwise you risk overkill."

What constitutes overkill? One example might be that of a small marketing firm that uses token authentication to grant users access, then requires two or three passwords to access network data, which is all encrypted. Another company might step over the security line into the overkill zone when it puts up firewalls to non-critical departments: Instead of protecting just its financial and R&D data, the company puts up an additional firewall between employees and administrative functions.

The importance of doing a thorough risk assessment and then matching solutions to vulnerabilities cannot be overstressed. Companies must identify which of their assets need protection, based on their business objectives. It is essential that the information technology staff be as familiar with the company's business objectives as it is with the corporate network.

To help users pinpoint areas most in need of security, Ed Sheehan, a principal at A.T. Kearney, a strategic technology consulting group in Annapolis Junction, Md., shares the risk-assessment procedure his company has worked up for its clients. "It's a balancing act and trade-off among the three A's: affordability, availability and appropriateness," he says.

First, Sheehan recommends, users must evaluate the information pertinent to their organization. "Make an evaluation of how important it is-extremely, moderately or not that big a deal," he says. "That understanding is critical to making the right security choice."

Next, review all potential threats to the company's operations and determine which are real and which represent groundless fears. Part of the discipline involves going through the whole catalog of known threats, opportunities for security breaches and any enabling technologies available.

This exercise not only rules out unlikely threats but identifies unprotected areas. "A false sense of security is more dangerous than thinking you're not secure," Sheehan says. He emphasizes that since there's no

perfect security, companies must focus on solutions that fix their problems.

The next step is to develop a security policy, which in turn will mandate how the network is set up. "You must have strong integrity checks to verify that what arrives is what was sent," says Sheehan. "The notion of integrity says that when information leaves the computer, if it is changed I can detect it."

Users should then review their network architecture, understand all viable threats and the appropriate preventive measures, then determine how much they can spend on security. Sheehan says a certain level of risk is inevitable, but each company must decide for itself how much risk is acceptable. Weigh the cost of a possible security breach against the cost of a solution. Precious security dollars should be aimed at weak spots in a network, not pumped into an across-the-board lockup.

Once users have identified their corporate risk and know which areas need protection, they must decide what kind of security measures to put in place. Overkill rears its head once again.

Reaching for a Solution

It's not uncommon for network administrators to reach for a solution that has worked well for them in other instances. For example, encryption may seem like a surefire way to protect data on the network. After all, a hacker hoping to break Data Encryption Standard-based private key encryption would have to go through 72 quadrillion combinations to decode the information, according to LeeMah.

Encryption may be a great idea in some cases, but it's also expensive, time-consuming and computer-intensive: Generating a private key with randomly chosen bits not only eats up your own computing resources, it adds minutes to the computing process. So, unless they're from the CIA, users should think again before encrypting everything they send across the network or type into a system.

"Encryption on a PC may not be the way to go because every time you open a file, you have to wait for it to de-encrypt," says Katherine Hutchinson, product manager at Harris Corp., Melbourne, Fla. "But a company should use encryption on a payroll datastream to a partner."

Instead of opting for link encryption, where everything that goes through a communications pipe is coded, a company may be better served by choosing a content-sensitive type of encryption that encodes only the information that most deserves it-say, financial data, confidential files, product formulas and codes. For information that needs to be scrambled only for short periods-an E-mail message, for example-using a different encryption key each time probably offers enough protection.

"But something like credit card data, which stays sensitive for a long time-meaning hackers can snare it and break it at their leisure-needs to be able to withstand a hacker's attempts for a very long time," Hutchinson says.

With the Internet assuming a more prominent role in business communications, much emphasis is being placed on firewalls, which screen system access and shield private networks from interlopers over the Net. "It became apparent with one of our banking customers that department firewalls were needed," says Hutchinson. "The individual who is authorized to order supplies for the bathrooms shouldn't have the ability to authorize a check."

She notes that many companies have installed firewalls to protect subnetworks (like that of the finance department) on their private networks. But some organizations misapply them by placing them between users and the departments and non-sensitive information they must regularly access. Rather than keeping

security threats at bay, these companies inadvertently prevent their own employees from accessing useful information.

Other companies have gone to great lengths to protect something like E-mail sent from the CEO to the chief financial officer through encryption-but fail to apply any type of protection to the word processing documents generated by those executives' secretaries, which often contain sensitive information.

"Nine times out of 10, senior management Is attached to the network and the documents they create are stored on a Novell network," says Robert Kane, co-founder of Intrusion Detection Inc., New York, a developer of software that Identifies shortcomings in a network's security.

"Hackers find out who the senior managers are from annual reports and who their secretaries are and which servers they're on. They find that some senior executives didn't want to use a password, or that the secretaries have all sorts of accessible word processing documents with sensitive information," Kane says. So the executives and possibly non-essential data are well protected, while the weak points-the executive assistants and secretaries-remain prime targets for major breaches.

Every security technology has an appropriate place. "You just have to match a technology to what you're trying to accomplish," says Harris' Hutchinson.

Oddly enough, security overkill also can be a by-product of security circumvention. Sometimes network administrators ignore the inherent security features found in products like NetWare-or, worse yet, they disable them.

Use Built-In Features

"Most companies don't know how to set them, or don't care, or don't have the time," says Intrusion Detection's Kane. In fact, employing a built-in security function generally means little more than changing settings or typing in affirmative answers when prompted during installation.

By not initiating built-In features, network managers force their employers to turn to additional security solutions-such as multiple passwords, token reauthentication and even encryption-to solve problems that don't exist, adding anywhere from tens of thousands of dollars to hundreds of thousands of dollars to a company's security budget.

"There's a tendency for people to believe that a network operating system is not secure," Kane says. Nonetheless, he says, network operating systems like Windows NT and NetWare have a certain baseline of security features. Windows NT, for instance, just received C2 certification, the lowest acceptable level of security required by the government. C2 certification encompasses security measures such as discretionary-access control and authentication, and identification. "That's a fairly reasonable level of security," he says.

And NetWare will lock out a user ID after three bad password attempts, Kane says. Nevertheless, Kane's organization found that 30 percent of the 250 companies it surveyed didn't have the option turned on.

"The LAN administrator says it's a pain in the neck, but what do they have to do? The feature suspends the ID on its own," Kane says, adding that administrators often admit it's less a question of inconvenience and more a matter of not wanting users calling to complain if the system locks them out. "But you can lock them out for just one hour," Kane says. "Here you are, getting free security, yet it's too much trouble to turn it on."

The costly tendency to ignore inherent security features in a wide range of high-tech products stems, in part, from the burgeoning responsibilities of the network administrator. Overworked and overstressed, the network administrator is hard-pressed to become familiar with the nuances of every software product on the network, and vendors often neglect to point out the security measures built into their products. In addition, information technology departments often view security as an entity that is completely separate from other IT functions.

Keep It Simple

Besides creating a false sense of safety, installing too many unnecessary layers of security may prompt busy users to find ways to circumvent them, exposing the system to all kinds of hazards and unauthorized access. Users who find security measures too cumbersome and time-consuming-for example, multiple sign-ons or misplaced encryption-may question the need for so much security and start looking for ways to short-circuit the process.

"You want security to be non-intrusive," says Intrusion Detection's Kane.

At Muhlenberg County Hospital, Plainfield, N.J., users must invoke a combination of access codes and passwords to get to sensitive information, according to the hospital's system analyst, Ludwig Erb. "We use an eight-character security code, then we have a login, and use a four-digit security code," he says. The hospital's combination of passwords and access codes could have become unwieldy, but the hospital's physicians and nurses don't see it that way because Erb and his department worked hard to make security a behind-the-scenes proposition. "The script file is doing all the work," says Erb.

Ty Berge, a network engineer at the Chicago office of Swiss Bank, who believes there can never be enough security, explains that the bank tries to make security "as transparent as possible, so the user doesn't even know a transaction is secure. Once they have to do too many things, people start trying to avoid using it," he says.

It's important to educate employees about the value of security. If a security policy is spelled out clearly, employees will understand what's expected of them and what the consequences of any breach might be, leaving no room for misinterpretation. If security measures are adopted that don't foist unnecessary hardship on employees, the chances of establishing effective system protection increase.

Granting Ownership

Security problems are compounded when the employees in control of a company's security have a myriad other duties. Security, while important, is maintenance-intensive and may be given short shrift. Or, to make up for the time they can't spend on security, employees might recommend more extensive security tactics, which starts a vicious cycle: More security means an even greater administrative and management burden.

This problem can be solved by giving sole responsibility to a single person or department (see page 71). Outsourcing security is another option for small companies and those that can't afford in-house security. An outsourcer can help develop, implement and monitor a security strategy. And, much like appointing a security officer, turning over the management of security to a third party essentially makes that party accountable, which, in turn, experts say, ensures greater protection of corporate assets.

In the end, remember: Security is crucial, but nothing guarantees a company 100 percent protection against electronic intruders, and no amount of paranoia can change that. Security overkill can destroy a company's livelihood and drain its assets. And that's the biggest danger of all.

Tech Tips

Security decision-makers can zero in on the options that best fit their organizations' needs by giving careful consideration to the following questions:

* Do we understand the value of our information? If we think we do, how do we know?

* Do we understand the information we have and how it is managed? Have we categorized that information-by users, processes, information objects and information flow-to its lowest manageable level?

* Have we assessed all possible threats and ascertained which threats are most relevant to our organization? Have we documented our protection requirements to safeguard our operations against those relevant threats?

* Does our information-protection policy take into account the nature of the information we want to protect, the security solutions available to us and the most efficient way to implement those solutions? Do we follow and enforce this policy? Do we manage it? Is it sufficient?

* Have we examined and evaluated solutions to our security shortcomings, or have we simply thrown hardware, software and procedural Band-Aids at what we perceive to be weaknesses in our system?

* Have we chosen appropriate products and mechanisms from a variety of vendors that interoperate well? Or have we let security-product vendors persuade us to accept a one-size-fits-all solution?

Have we adopted a proactive approach toward building in appropriate security measures? Is that approach based on a comprehensive understanding of our security requirements?

Source: A.T. Kearney

Secure-Speak

Authentication: A process to verify the identity of a user, device or other entity; often, a prerequisite for access. Types of authentication methods include challenge/response, whereby one device initiates a numerical challenge to another, which, in turn, generates a numerical response that must match a predetermined scheme; and time-based, response-only authentication, which uses a proprietary algorithm to generate time-stamped passwords.

Encryption: The mathematical process of encoding information to protect it from unauthorized use.

Firewall: A software-based solution that erects security shields between the more public parts of a network, where users roam freely, and those subnetworks housing more sensitive information that is accessible only to authorized users.

Password: Typically, a string of one to 10 alphanumeric characters that grants access to a system. To be an effective security device, a password must be known only to its authorized user.

Personal authentication device: A portable or fixed device that provides precise identification and validation of each user; also called a token.

User ID: A symbol or character string that uniquely identifies a specific user to a computer system.

Sources: LeeMah DataCom Security Corp., CommunicationsWeek

A New Breed of Security Officer to the Rescue

A network manager often is overextended and overstressed enough without the full-time job of security falling under his/her domain. Increasingly, companies are easing the network manager's load by moving security responsibilities to a specific person or department assigned the task of focusing strictly on the development and administration of a comprehensive security policy.

The upshot not only is a happier network manager, but also tighter security, greater accountability, less likelihood of security overkill and better management of network-security measures, says Mich Kabay, director of education at the National Computer Security Association, Carlisle, N.J.

What qualities should a security officer possess? Here's Kabay's profile of the perfect candidate:

* Look for a high-level manager. When a company creates a security-officer position, it should appoint someone who already is a member of the senior management staff. Your first security officer should wield authority based on experience, and should be known and liked by other senior management officers. Your security officer should possess sound business acumen.

* Seek someone who can roll with the punches. A good security officer is non-authoritarian. In Kabay's view, it's a big mistake to put someone in the position who considers a disagreement an invitation to do battle. Find a security officer who can tolerate ambiguity and frustration-preferably someone who is outgoing and people-oriented, since this person's main task will be to convince his or her coworkers that security matters. Your security officer must be able to focus on people's needs while managing not to worry unduly about winning short-term approval or personal popularity contests. There's a difference between being flexible and non-authoritarian and being a spineless wimp, Kabay says.

* Identify a candidate with technical know-how. Any security officer who's up-to-date on technology will enjoy a big advantage in promoting a security policy, says Kabay, noting there is nothing worse than a user who knows more about the company's technology than the security officer.

According to JoAnn Perry, principal at JoAnn Perry & Associates, Sparks, Nev., and formerly the security officer for nearly a decade at New York investment firm Goldman, Sachs & Co., understanding the company's business policy is just as important as understanding its technology.

"If you ignore that, that's how you fail," she says. Non-business-savvy security officers get caught up in issues that ultimately aren't that important, she adds. "They entrench themselves over security issues they should not entrench over," she says, and too many warnings of inconsequential security problems fall on deaf ears. "It's like the boy who cried wolf," she says.

Topic

Management Issue
MIS
Network Management
Data Security Issue

Record #

17 781 212

CommunicationsWeek

CommunicationsWeek Sep 16, 1996 n628 p174(1)

Security Dynamics' web authentication.

(Network security software restricts web access)

Author

Fontana, John

Abstract

Security Dynamics Technologies Inc introduces the $2,450 Ace/Server for Windows NT, the $149 Ace/Client for Windows NT, and the $34 Security Dynamics Technologies SecurID cards. The Ace/Server network security software lets network administrators restrict access to the World Wide Web on a per page basis. Ace/Client will prompt the user upon entering a secure web page. Upon entering a password and the code from the SecurID card, access will be allowed to the secure sections. Both the Ace/Server and Ace/Client work together in verifying user authorization. These three products are the are the first results of a joint licensing agreement between Security Dynamics and Microsoft. All three products run on Windows NT.

Full Text

Security Dynamics Technologies Inc. Is scheduled to announce this week technology for user authentication that lets network administrators in Microsoft Windows NT environments restrict Web access on a page-by-page basis.

The Cambridge, Mass., company also announced Windows NT support for its network security software, Ace/Server, previously available only on Unix platforms.

Web-page authentication is provided via software for both clients and servers, as well as through Security Dynamics' SecurID card, a small piece of hardware that provides numerical codes. The product is the first direct result of a joint licensing agreement between Security Dynamics and Microsoft (CommWeek, Sept. 2).

Ace/Client for Windows NT will include a WebID feature set that allows user authentication through SecurID for individual Web pages or directories of pages. When a user encounters a secure Web page, he will be prompted for a password and the six-digit code shown on his SecurID card. Authentication is verified by Ace/Server and the user is granted access. Authentication only needs to take place once per session. Audit and logging management is integrated with Microsoft's standard Internet Service Management interface.

In keeping with its Microsoft agreement, Security Dynamics will initially make WebID available only for the Windows NT 4.0 environment. Eventually, a variety of platforms and browsers will support the feature set.

The company also announced Ace/Server for Windows NT, which works in conjunction with Ace/Client to authenticate users. It Integrates the security features of SecurID and SoftID authentication and security management into the Windows NT environment, the company said.

"This is a continuation of our relationship with Microsoft and a reaction to our customers' demand for Windows products," said Eric Ogren, product manger at Security Dynamics.

Analysts said the move made marketing sense, but it may have a short shelf life because of impending advances in security technology. "This move shows a consistency and is the right direction from a

marketing perspective, but it's not a revolutionary announcement from a technology standpoint," said Gary Lynch, research director of information security strategies at the Gartner Group Inc., Stamford, Conn.

Ace/Server costs $2,450; the Ace/Client, $149. SecurID cards cost $34. The products are scheduled for release next month.

Security Dynamics can be reached at 800-732-8743.

Type

Product Announcement

Company

Security Dynamics Technologies Inc.

Product

ACE/Server for Windows NT RAS (Network security software)
ACE/Client for Windows NT RAS (Network security software)
Security Dynamics Technologies SecurID (Data security device)

Topic

Networking Software Product Introduction
Network Security Software
Data Security Device

Record #

18 700 545

CommunicationsWeek

CommunicationsWeek Sep 2, 1996 n626 p26(1)

Increased access to encryption.

(Microsoft, Security Dynamics Technologies, RSA Data Security sign cross-licensing agreement) (Company Business and Marketing)

Author

Fontana, John

Abstract

Microsoft, Security Dynamics Technologies and RSA Data Security have signed a cross-licensing agreement that will provide network mangers with access to the latest encryption technology. Security Dynamics' and RSA's security technologies will be tightly integrated with Microsoft's products to develop an environment where software developers can have access to standardized cryptography. The agreement revolves around Microsoft's CryptoAPI (CAPI) technology, the basis of Microsoft's Internet Security Framework. CAPI allows third-party vendors to add encryption and cryptography to programs via a single API. Microsoft has licensed CAPI to RSA in exchange for inclusion in RSA's BSAFE tool kit, which permits users to develop CAPI-compatible programs for Windows. Under the agreement, RSA can make CAPI available on several platforms.

Full Text

Users setting up electronic-commerce installations on Microsoft platforms will now have easier access to leading security technologies, thanks to a cross-licensing deal between Microsoft, RSA Data Security Inc. and Security Dynamics Technologies Inc.

The immediate benefit for network managers will be multi-level user access management and the availability of the latest encryption technology.

"What we are doing is a tight integration of RSA's technology and Security Dynamics technology with Microsoft products to create an environment where developers can have broad access to standardized cryptography," said Jim Bidzos, president of RSA.

The announcement centers on Microsoft's CryptoAPI (CAPI), which lets third-party vendors add cryptography and encryption to applications through a single API. CAPI is the foundation of Microsoft's Internet Security Framework, a set of technologies for electronic commerce and communication that support Internet security standards.

"In the next year or two, CryptoAPI should be the de facto standard for operating systems and applications," said Marlo Kosanovich, a research analyst with the Reston, Va.-based META Group. "The area where Microsoft can win in the security market Is where they're strongest:at the operating system and application level.

"This won't drive electronic commerce directly, but it helps in some areas," Kosanovich explained.

Brad Silverberg, senior vice president of Microsoft's Internet platform and tools division, said Microsoft has licensed the CAPI technology to RSA for Inclusion in its BSAFE tool kit, which will let users produce CAPI-compatible applications for Windows platforms. The license also lets RSA make CAPI available on a variety of platforms, which Microsoft hopes will lead to the development of cross-platform applications and

support for Internet standards.

RSA will provide assistance and licensing rights to assure its latest technology is available in Microsoft's operating systems and products. Microsoft, which uses RSA technology as the cryptographic engine for CAPI, will provide source code to RSA for the development of a suite of cryptographic engines.

"The important thing is that developers can now write to a single API," Bidzos said.

CryptoAPI 1.0 is now shipping for Windows NT 4.0 and Internet Explorer 3.0, with 30 cryptography function calls, including digital signatures. The next version of CAPI, scheduled for beta testing later this fall, will integrate certificate management into the NT administrative model.

The only catch seems to be that the security benefits are available solely to NT and Microsoft Internet Information server users, a fact not lost on Microsoft's competitors.

"In terms of multiplatforms for CAPI, you can forget it," said Eric Greenberg, Netscape Communications security group product manager. "This CAPI approach is an incomplete approach."

Microsoft plans to incorporate Security Dynamics' SecurID tokens and ACE/Server authentication products into Windows NT products and Microsoft's Internet Information Servers. This will give network managers multilevel user access management on workstations, servers and intranets.

"This gives us a platform to build on for future security releases," said Charles Stuckey, CEO and chairman of Security Dynamics, which purchased RSA in July.

John Evan Frook contributed to this story.

Company

Microsoft Corp.
RSA Data Security Inc.
Security Dynamics Technologies Inc.

Product

CryptoAPI (Systems/data security software)

Topic

Company Licensing Agreement
Encryption
Systems/Data Security Software

Record #

18 666 994

Worldwide Information Systems

Bull

Bull CP8 Technologies

ALLIANCES PATENTS HELD

STANDARDS SMART CARD PRIMER

SECURITY PRIMER SMART CARD 2000

original & extra set

[illegible]
VAR PROGRAM
[illegible]
SOLUTIONS
REFERENCES
PRODUCTS
CONTACT US

Bull CP8 and the smart card technologies

With more than 20 years experience in the research, development and deployment of secure transaction solutions based on smart card technologies Bull CP8 is a recognised leader world-wide.

Since their in invention in 1978 by Motorola and M. Ugon of Bull CP8, our technology leadership has been beyond question. With more than 850 patents filed on related inventions and our smart card operating systems sublicensed world-wide, we are clearly in the best position to talk about the technologies behind the chip.
The security that Bull CP8 smart cards bring stems from our unique and original monolithic architecture and our operating systems or masks.

The cryptology algorithms supported by the masks let you perform the whole range of security functions.

Standards and market forces

Knowing how important standards are to its customers, Bull CP8 offers a range of cards and devices that meet the ISO standards many of which CP8 was either the originator or participated in the definition. In addition Bull participates in and respects the recommendations of many other market led standards such as those of Mastercard and Visa around the Secure Electronic Transaction as well as participating in the definitions of the next range of universal bank cards working under the name of EMV (Europay, Mastercard, Visa).

Bull CP8 Products

SMART CARDS SST OFFERS

READERS/ENCODERS EFT TERMINALS

SECURITY PRODUCTS RETAIL TERMINALS

CONTACT US

Introduction

Bull CP8's history in smart cards goes back to their inception in 1979 when, in collaboration with Motorola, Michel Ugon of Bull CP8 produced the world's first micro processor card. Since then we've gone on to leverage this technology advantage through the deployment of world beating products:

- □ Bull CP8 is the world leader in smart card operating systems with over 60% of all chip cards sold based on Bull CP8 technology. More than 120 million Bull CP8 ________________ are in use world-wide and we supply the most successful Electronic Purse card in the world with more than 10 million cards being distributed across Europe and beyond.
- □ CP8 is the worlds third largest supplier of ____ and the number 1 in Europe.
- □ More than 15,000 Bull CP8 Automatic Teller Machines and _________________ have been installed world-wide from our extensive baking offer.
- □ Bull CP8's technology research in the smart card ____________ domain has resulted in sales of over 300,000 products across the world.
- □ Our extensive knowledge of the world of EFT-POS has led to the introduction of new _____ _______________ already smart card enabled.
- □ Bull CP8's extensive experience in the security domain is now being extended to ____________ _______ for sale to the commercial world.

ecash about ecash

Cash on the Internet now has become reality with ecash.

- □ Introduction
- □ The ecash concept
- □ Ecash today see the page about the ecash trial
- □ Ecash tomorrow
- □ Further reading see the articles An introduction to ecash and Money on the Internet and the ecash FAQ.

Introduction

Ecash is designed for secure payments from any personal computer to any other workstation, over email or Internet. Ecash has the privacy of paper cash, while achieving the high security required for electronic network environments exclusively through innovations in public key cryptography. In the past DigiCash has pioneered such cash for chip cards and electronic wallets, always with a tamper-resistant chip for storing the value. Now we present the first software only solution: ecash.

With ecash you can pay for access to a database, buy software or a newsletter by email, play a computer game over the net, receive $5 owed to you by a friend, or just order a pizza. The possibilities are truly unlimited.

The ecash concept

With the ecash client software (short: client) a customer withdraws ecash (a form of digital money) from a bank and stores it on his local computer. The user can spend the digital money at any shop accepting ecash, without the trouble of having to open an account there first, or having to transmit credit card numbers. Because the received ecash *is* the value involved with the transaction, shops can instantly provide the goods or services requested.
Person to person payments can also be performed with ecash.

Ecash and security

When using ecash, your cash flows to its destination over the Internet (or any other computer network). The open architecture of the Internet requires security measures to be taken against attempts by unfriendly third parties to intercept the digital money. Ecash provides the highest security possible by applying public key digital signature techniques.
Additional security features of ecash include the protection of ecash withdrawals from your account with a password that is only known to you; not even to your bank.

Ecash and privacy

One of the unique features of ecash is *payer* anonymity. When paying with ecash the identity of the payer is not revealed automatically. This way the payer stays in control of information about himself. During a payment a payer can of course identify himself, but only when he chooses so.
Ecash offers one-sided anonymity; when clearing a transaction the *payee* is identified by the bank.

Read more about the technique behind ecash's security and privacy on the ecash security and privacy page.

Ecash and crime

It may seem that the privacy offered by ecash can be misused by criminal elements. However, because the privacy is only one-sided and a set of regulatory measures can be taken, ecash is not the ideal tool for criminals.
Read more about this on the ecash and crime page.

The ecash client software

Ecash works on all major platforms (MS Windows, Macintosh and UNIX). The graphic user interface works with a small comprehensive status window displaying the amount of money in cash. A text mode version is available for people without a graphical operating systems.
If an online ecash accepting shop requires payment, depending on user settings, the client will handle the transaction completely by itself, or prompt the user for authorization.
For the current version of ecash a network connection is required, but a version that will work through email will be available in the near future.
To see how it works read the about the client software page.

Accepting ecash

Part of the ecash concept is a very low threshold for shops to start accepting ecash. In our view the Internet is the ideal infrastructure for big players as well as numerous small shops offering a wide variety of specialized goods and services. In fact, any user can accept ecash payments sent on- or off-line.

Ecash today

The Cyberbucks trial

Today, almost 30.000 people are using ecash in our world wide trial. The digital money used in the trial, the *Cyberbuck*, can not be exchanged for real money, but valuable goods and services can be purchased in more than one hundred shops that have joined the trial and accept ecash cyberbucks.

The trial, which started in October 1994 and was closed for new testers a year later, introduced cash in cyberspace and created an enormous amount of interest from users, shops and banks as well as the media.

The trial is officially closed for new testers, but if you're interested in starting an ecash accepting shop or if you have other good reasons why you should be able to participate in the trial, please email to our trial coordinator to ask for an account. The ecash trial shop software is available for free, and full support is given to new online shops. With the introduction of the *remote shop server*, starting a shop has become even easier.

For more information read the ecash trial page.

Real banks

The first banks have started issuing ecash denominated in real currencies. Check at the ecash issuers page

for up-to-date information, including instructions on getting accounts and software.

Ecash tomorrow

Although DigiCash is running an ecash bank in the trial, *we* do not intend to start an exchange between Cyberbucks and other currencies. A growing number of banks, financial institutions and other organizations are very interested in issuing ecash, and we have sold several ecash licenses. DigiCash currently follows a non-exclusive licensing policy, allowing multiple parties to issue ecash with their own, competitive, pricing structure.

Further reading

Ecash concepts are explained in more detail in An introduction to ecash.
Ecash is compared with other payment methods in the article Money on the Internet.
Frequently asked questions about ecash are answered in the ecash FAQ.
You can find more information on the DigiCash publications page.

ecash digicash home

products smart cards

DigiCash, a world wide leader in smart card mask development

- □ Background
- □ Proven technology: the SAKE card, see the SAKE page
- □ Technology breakthrough: Blue, see the Blue page
- □ Smart card production, see the smart card pictures page

Background

From the day it was founded, DigiCash has been developing its smart card mask technology.

For its own products, DigiCash has developed many smart card masks, with each new generation improving upon the technology of the previous one. After mask generations with the code names Grey, Yellow, Green, and Purple (product name SAKE), we have now developed the Blue smart card mask.

Furthermore, DigiCash has done smart card mask development for many other projects it was involved in, such as the CAFE project.

DigiCash offers a full set of development tools to help you develop your own smart card mask.

Proven technology - the SAKE card

Where other cards force the use of protocols fixed by the cards vendor and require an application to be based on a specific file-organization model, the Sake card allows the design more flexibility.

The application is programmed into the Sake card itself and doesn't have to operate from the card reader alone, so there is a better grip on the functionality and security aspects. Custom protocols or security measures can easily be implemented partly own to the ability to verify RSA signatures.

For more information visit the SAKE page.

Technology breakthrough - Blue

Public Key Debit allows off-line secure payments without tamper-resistant terminals. Each of the payments uses a unique public key signature in a way that allows thousands of payments between two reloads.

For more information visit the Blue page.

Smart card production

Our licensees can buy our chips directly from multiple suppliers of silicon, such as Motorola and Thompson. The chips can then be made into cards by any one of more than a dozen companies around

the world today.

Some of our cards can be seen at the Smart card pictures page.

products digicash home

products road toll

The toll payment/road pricing technology everyone has been waiting for...

- □ Background
- □ DigiCash, the ideal development partner
- □ Features of our technology
- □ Applications of the technology: see DyniCash and The Rijkswaterstaat project

Background

In 1990 DigiCash performed a proof of feasibility for the Dutch Ministry of Transportation and Infrastructure on an automatic road pricing system. This project ended successfully (see The Rijkswaterstaat project .)

When the Netherlands abandoned plans for realizing road pricing, DigiCash took the development of the system, under its own funding, from proof of feasibility to the next stage which included fabrication of actual chip cards and various readers. Then Amtech licensed the DigiCash technology, and it was developed further to interface to their microwave and controller technology. This development has resulted in the DyniCash system. It has been extensively tested, and is being marketed by Amtech.

Our road toll technology is platform independend and licensed on a non-exclusive basis.

Road toll development by DigiCash

DigiCash is truly the ideal partner in development of road toll systems and applications.

Expertise

After having been involved in the early days of creating requirements and actually building the first smart-card-based road pricing system, we have gained a good deal of knowledge in this specialized area. Moreover, we are acknowledged as world-wide leaders in electronic payment technology, and particularly for any applications involving user privacy.

Development Support

DigiCash can offer its licensees a full range of support, including basic technology transfer and access to future improvements. The capabilities of DigiCash extend, should they be required by a licensee, all the way to complete technical interfacing efforts for digital hardware and software as well as for custom smart card masks.

Software

We have a complete set of software for road toll systems, including IVU, roadside equipment, and plaza computers. It runs on various platforms, including a complete simulation we built to allow easy testing and integration of the system.

High-Speed Crypto Hardware

To allow ultra-fast processing of transactions, we developed modular high-speed encryption devices that are available from us and are produced as a second source by Crypto AG, the world-wide market leader in cryptographic equipment. For more information on our encryption devices see the Mask development and and encryption tools page.

Use of our smart card chips

DigiCash has established itself as an independent leader in smart card mask technology. Read more about our mask development on the smart card page.

Patent Licenses

We have an extensive patent portfolio in the area of electronic payments, particularly where privacy, smart cards, and high-speed are concerned.

Technology features

Our technology includes the following major features.

Privacy

Our patented approach is the only one that can allow a secure payment from an ic card while keeping the roadside equipment from identifying the card. (See the article "Achieving Electronic Privacy".)

Speed

A complete transaction, from detection of the IVU to final acceptance of the payment by the roadside equipment takes only 20 milliseconds.

Flexibility in configurations

Both pre- and post-payment options are available from the same or different cards, and can be used in any combination of open or closed tariff structures.

Public Key Security

Our unique signature transporting approach provides true public-key cryptographic signatures at speeds suitable for highway use. Such signatures are generally agreed as needed for large-scale prepaid or stored value smart card systems, especially where co-operation between multiple issuing banks is envisioned. (See the article "Prepaid Cards Compared".)

Applications of the technology

- DyniCash
- The Rijkswaterstaat project

[illegible] digicash home

INFORMATION

Payment System Summary (Buying and Selling)

The First Virtual Internet Payment System provides a simple, secure and safe method for buying and selling over the Internet. No special hardware, software or encryption is required. All you need is ordinary e-mail!

With First Virtual, you use a VirtualPIN (an alias for your credit card) to make purchases. Your credit card number is **never** transmitted over the Internet!

As added security, every purchase you make is confirmed via e-mail!

To Become A Buyer

- □ You must have:
  - □ Internet e-mail.
  - □ A valid Visa or MasterCard.
- □ Then complete an application and receive your VirtualPIN (IMPORTANT: As part of the process you will register your credit card with First Virtual over the telephone, **not** over the Internet!)

To Buy

1. Give your VirtualPIN to a seller instead of a credit card number.
2. First Virtual will then send you e-mail to confirm the purchase. Answer the message with:
   - □ "yes" to confirm the sale.
   - □ "no" to cancel the sale.
   - □ "fraud" to immediately cancel your VirtualPIN (it is being used without your consent!)
3. If you confirm the sale, your credit card is charged by First Virtual **completely off the Internet!**

Shopping links: The InfoHaus and Independent Merchants Accepting First Virtual

To Become A Seller

You must:

- □ Have a bank account that accepts direct deposit (via the US ACH system).
- □ Complete an application
- □ Send a check to First Virtual for the $10.00 registration fee.

To Accept Payment

1. A buyer sends you a VirtualPIN, which you may easily verify as valid.
2. You send a message to First Virtual containing the buyer's VirtualPIN and the amount of the sale.
3. When First Virtual confirms the transaction with the buyer, you are notified via e-mail.
4. Later, the amount of the sale (minus First Virtual's fees) is deposited directly into your bank account!

This is an abbreviated overview. Please refer to Selling - complete details for more information.

Apply | Shop | Help | Information | What's New?

Comments about this Web site: webmaster@fv.com

INFORMATION

[Clickable Map] [Text Index] [Home Page]

Buying -- complete details

Buying over the Internet using your VirtualPIN is easy, safe, and convenient.

Contents of This Page:

To Become A Buyer

You need:

1) Internet E-Mail

The First Virtual Internet Payment System requires that you have a private (not shared with anyone else) electronic mail address capable of sending and receiving messages over the Internet. For further information, consult Will My E-mail Address Work With First Virtual?

All communications between you and First Virtual will take place through this private address, including when you confirm purchases and authorize First Virtual to charge your credit card. For security reasons you should not share this e-mail address with anyone!

(IMPORTANT: When changing e-mail addresses, you need to inform First Virtual BEFORE closing your old e-mail account. **For security reasons, our confirmation message must be sent to your old address.**)

2) A Valid Visa Or MasterCard

(NOTE: A Visa or Mastercard debit card is also acceptable -- ask your bank if it offers this service.)

Step 1: Complete An Application

You may Complete An Application via the Web or by:

□ E-mail to "apply@card.com"
You will automatically receive a reply message containing a form to fill out. Send the completed form to "newacct@card.com"

- □ Telnet to "telnet.card.com "
  When you connect, login as "fv". Follow the on-screen instructions and complete your application interactively (any Telnet connection will work, but X-Windows users will be able to use a graphical interface to fill in the form).

Among other things, the application will ask for two things:

1) Your "Full Name"

This is the name that sellers will see when you purchase something over the Internet. It will be public information. You do not have to use your actual name -- a business name, nickname or pseudonym is acceptable.

2) Pin Choice

This is your preliminary choice for your account ID. It must be a minimum of 8 characters in length and made up of letters and / or numbers. Pick something easy for you to type and remember, but hard for other people to guess. It should NOT be your "Full Name", a password used on any computer system, or any other secret information (such as the PIN for a bank card).

First Virtual will create your **final account ID, called a VirtualPIN**, by adding a prefix of letters or numbers and a hyphen to the beginning of your PIN choice. (NOTE: The addition of the prefix is for security -- it guarantees that your VirtualPIN will be unique.) You will be sent your completed VirtualPIN via e-mail shortly after you complete step 2 (Activate Your Account). When making purchases, you will **use your VirtualPIN as your account ID, not the PIN choice you specify on the application.**

Step 2: Activate Your Account

After completing your application, you need to activate your account by registering your credit card number with First Virtual.

An e-mail message will be sent to you containing a telephone number (toll-free for U.S. users) and a 12-digit application number. This application number is the number you will use to identify yourself when you call.

When you call First Virtual, enter the 12-digit application number, your credit card number and its expiration date. You may call anytime, day or night.

If you encounter problems (for example, if our system does not appear to understand your telephone's tones), please send an e-mail message to "humanhelp@fv.com" (DO NOT include your credit card information in your e-mail message!). A First Virtual operator will contact you to get your credit card information by other means.

Step 3: Receive Your VirtualPIN

After registering your credit card, you will receive an e-mail message from First Virtual containing your VirtualPIN! (This generally takes less than 2 hours, but it may take up to 24 hours.)

You are now ready to buy!

Fees

There is a $2.00 annual fee to have a VirtualPIN. The fee is charged to your credit card when you become a Buyer and on the anniversary of your registration.

What You Can Buy

You may buy *anything* with your VirtualPIN -- goods, services, information products, memberships and more.

Information Products

Currently, information products are the most common things sold on the Internet because they can be ordered, delivered and paid for on-line. Information products include software, graphics, newsletters, on-line publications and anything else you can download to your computer.

"Try before you buy"

In keeping with the Internet's history of open information exchange, most sellers will allow you to download and review an information product before deciding if you want to keep it and pay for it. Sellers are not required to do this, but most of them do.

To Buy

Give your VirtualPIN to a seller instead of a credit card number.

You may generally download "try before you buy" information products as soon as you give your VirtualPIN to a seller. Other sellers will wait until you confirm the sale with First Virtual before delivering products, activating your membership, etc.

First Virtual will then send you e-mail to confirm the purchase.

The message will include the seller's name, your "Full Name," the price and a description of the product.

If you are using our Electronic Mail Extension Software, a convenient form explaining the purchase will appear, allowing you to reply automatically.

Reply To The Message With:

□ YES to confirm the sale.

By replying "yes", you are authorizing First Virtual to charge your credit card for the purchase. Charging your credit card takes place completely off the Internet. For "try before you buy" products, a "yes" answer means that you have received the information product, examined it, and feel it is worth paying for.

□ NO to cancel the sale.

By replying "no", your credit card will not be charged. You may cancel the sale for many reasons: the information product may not be what you wanted, does not work on your

machine, or the downloaded file is corrupt; perhaps you changed your mind about the hard good you ordered and do not want it shipped. Whatever the reason, you have the right to reply "no" and cancel the sale.

(Important: Replying "no" is a privilege of our system. Users who abuse this privilege may have their VirtualPINs canceled. Please consult our Terms and Conditions for more information on the legal agreement you have with First Virtual regarding "no" responses.)

- □ FRAUD to immediately cancel your VirtualPIN.

  A "fraud" answer means that you believe your VirtualPIN has been stolen. Answer "fraud" only if you did not make the purchase you are asked to confirm. Canceling your VirtualPIN is permanent -- it cannot be used or reactivated for any reason. If you want to continue using First Virtual, you must apply for a new VirtualPIN. This is a fundamental security feature of the First Virtual system.

Your reply is sent to "response@card.com" and should only contain one of the above words: "yes", "no" or "fraud" (except in the case of "help" as explained below).

If you need help

When asked to confirm a purchase, you may reply with the word "help" by itself on any line with a description of your problem starting on the next line. The text that follows the word "help" will be forwarded to a customer service operator who will respond to your problem personally.

How Your Credit Card Is Charged

Your credit card will be charged for any purchases you make, by First Virtual, completely off the Internet. Multiple purchases are often "bundled" and posted to your credit card as a single item.

Before your card is charged, we will send you a "payin notification". This is an item-by-item listing of the purchases you have made, the total, and a code number that will appear on your credit card statement.

```
Example:

  You, Joe X. Ample, previously approved the following purchases:

  Amount   Seller/Description
  ---------- ------------------
         0.50 First Virtual Photos
                 Inside_the_Park
         0.50 First Virtual Photos
                 Feeding_a_Giraffe

   We have NOW billed your credit card for these PREVIOUSLY APPROVED
   purchases, for a total of 1.00 (usd us dollars).

   This line charge may be identified as "100076044"  on your
   credit card bill.
```

When you receive your monthly statement from your credit card company, it will only show the

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

code and the total, not each individual purchase.

```
Example:  INTERNET 1ST VIRTUAL   100076044     $1.00
```

Be sure to keep your "payin notifications" (itemized listings) to understand every First Virtual charge to your credit card.

Refunds

If you are not satisfied with, or did not receive a purchase, please contact the seller directly to resolve the problem or issue you a refund. The seller's Web site should provide an e-mail address for customer support.

If you cannot reach an agreement with the seller, you may send an e-mail message to support@fv.com to request that First Virtual issue you a refund. Be sure to include the seller's e-mail address and an explanation of the situation, including why the seller did not handle the refund directly. (NOTE: If First Virtual issues you a refund, your VirtualPIN may be suspended.)

Shopping With Your VirtualPIN

To find shopping sites, start by following the Shop link at the bottom of every page on our Web site. There you will find links to the InfoHaus (our on-line mall for information products) and to a partial list of independent merchants who accept First Virtual. Internet Search Engines like Yahoo, Lycos and Alta Vista are also effective ways of finding First Virtual merchants.

To Change or Close Your Account

You may **change (or cancel) your account** via:

□ Telnet to "telnet.fv.com". Login as "fv", then choose "change" from the menu and follow the on-screen instructions. This interactive system is the easiest method to make changes.

□ E-mail to "initchg@card.com" with your VirtualPIN in the subject line. You will automatically receive a form and instructions for changing your account via e-mail.

You may **close your account** via:

□ E-mail to "closeacct@card.com" with your VirtualPIN in the subject line.

Before any change to your account becomes permanent, we will ask you to verify it by responding "yes" to a confirmation e-mail message.

(IMPORTANT: When changing e-mail addresses, you need to inform First Virtual BEFORE closing your old e-mail account. **For security reasons, our confirmation message must be sent to your old address.**)

Why First Virtual Is Safe

With First Virtual, you use a VirtualPIN (an alias for your credit card) to make purchases. Your credit card number is never sent over the Internet. Instead, you register your credit card with First Virtual over the telephone. It is protected with the same care and by the same mechanisms as banks use.

It is safe to send your VirtualPIN over the Internet because, even if it were stolen, a criminal could not use it. Every charge to your credit card must be confirmed from your private e-mail address; your reply of "fraud" would immediately, and permanently, cancel your stolen VirtualPIN!

Your VirtualPIN also reveals nothing about you. No one can discover your postal address or phone number by knowing your VirtualPIN. Sellers are only told your "Full Name" as provide on you application (so we can refer to you without sending your VirtualPIN over the Internet more often than is necessary). Remember, your "Full Name" does not have to be your real name -- it can be a business name or a nickname.

For more information on First Virtual and security, please refer to our Frequently Asked Questions.

Apply | Shop | Help | Information | What's New?

Comments about this Web site: webmaster@fv.com

Gemplus Microprocessor Cards

Return to Home Page

Smart cards offer a simple and convenient way to handle permanently and securely various pieces of information, which can be locally treated and managed thanks to the cards' 'on-board' intelligence.

Independent and Self Secure

Many applications such as banking, physical access control and computer access control, portable files, require a high level of security. By offering the ability to perform a complete and local authentication of the card's holder, microprocessor cards can operate off-line. Benefits are shorter connection times, enhanced security since no sensitive information is sent over the network, and lower operating costs.

Multi-Applications

Gemplus microprocessor cards offer multi-application facility: this means that different services offered by different providers can share the same card, by using independent access control and security features.

From Concept to Product

Our customers have expressed the need for a powerful, easy to use, and universal operating system dedicated to smart card applications. Gemplus software and design engineers came up with the right answer: the C.O.S. or Chip Operating System. This Operating System has been ported on to the complete Gemplus microprocessor card family, both EPROM and EEPROM. Upward compatibility is fully ensured: this enables our customers who already have applications running with our cards to switch to the newest Gemplus product without having to make major developments.

Microprocessor Cards Overview

Gemplus offers a full range of microprocessor cards which are built around an 8 bit core with different memory sizes, for:

- ROM (Read Only Memory),
- RAM (Random Access Memory), and
- EPROM (Electrically PROgrammable Memory),
- EEPROM (Electrically Erasable and PROgrammable Memory).

Gemplus microprocessor cards also integrate cryptographic* functions for applications requiring a high level of security. The M.C.O.S, or multiple directory COS is also available now. This is an enhanced version of the Chip Operating System allowing creation and management of several independent directories within one smart card. Gemplus can also develop dedicated routines which can be electrically programmed into the EEPROM area to further extend the card processing power.

Security

Gemplus cards are manufactured in a highly secured environment, complying with banking

authorities' requirements. Tight controls are implemented throughout the manufacturing process, from chip transportation to card delivery. The integrated circuits used by Gemplus have built-in security features such as fuses, transport codes, application codes, security detectors.

Card Printing

The Gemplus four colour printing process enables the reproduction of company logos, texts, photographs and drawings with an excellent resolution and a good reproduction on both sides of the cards. This highly flexible equipment is suitable for quantities ranging from a few thousand to millions of cards.

Card Personalization

An electrical personalization can be performed at Gemplus premises, for example to load inside each card custom files and directories, access conditions and identification numbers. A graphical personalization can also be performed in parallel, with a possible link between graphical and electrical information.

Quality

Today, two quality protocols have been signed with France Telecom according to ISO 9002. In 1995, following ISO 9004 model, a global quality management will be operational for the entire Gemplus Group based on employees, skilled and highly motivated. The product is tailored to your needs, and the quality of service meets your requirements.

Smart Card Environment

Gemplus provides its customers with a complete range of hardware and software tools to develop smart card applications. These are:

- Card readers and drivers,
- Electrical and graphical personalization tools,
- Software programs for card evaluation and programming, such as PILOT and COSSACK.

Specific developments are also possible on request.

Standard compliance

Gemplus technical staff participates heavily or even leads several standardization committees such as ISO, AFNOR, and ETSI. New products under development will comply with emerging standards in order to guarantee to our customers a full compatibility between Gemplus smart cards and their environment, present and future.

Please note that availability of full cryptographic features is submitted to agreement of National Security Agencies.

Return to Home Page

Last updated 1st April 1996

Gemplus Smart Card Readers & Couplers

GEMPLUS

Return to Home Page

GCI400:Smart Card Coupler
GCR400: Smart Card Reader
GCR400-FD: The PC-Integrable Smart Card Reader
Gemplus' hardware know-how
GPR400: Compact Smart Card Reader (PCMCIA format)

Gemplus offers a full line of smart card readers. These devices are designed around a modular unit: the GCI400 mini-coupler. Gemplus coupler and card readers allow users to easily implement and manage the interface between the world of smart cards and that of computer systems

The most recent smart cards require high-performance, user-friendly card readers. By designing its systems around the GCI400 modular mini-coupler, Gemplus is able to offer an extensive product line capable of meeting all users needs. These smart card readers provide a solution that will be tailored to your environment, for applications ranging from electronic payment to access control, not to mention telecommunications, vending machines, customer loyalty...

GCI400: The Central Unit

Our different card readers are designed around the modular architecture of the GCI400 (Gemplus Card Interface) device and its OROS (Open Reader Operating System). The GCI400 is a compact, modular and upgradeable device. Its electronic system is fitted with the different hardware and software components necessary to manage the interface with the smart card. The mini-coupler includes the full range of high-performance interface functions: power supply, data exchange, selection of protocol for external communications, connection of extension cards.

The GCI400 is an all-purpose coupler:

- for integration in payphones for all types of telecom applications
- central element in payment terminals for all payment or electronic purse applications
- interface with other devices for automatic vending applications
- central component for dedicated access control (physical or logical) applications...

See a photo of the GCI400 smart card coupler (24K bytes)

The GCI400 is designed around OROS, an advanced operating system. Its main advantage resides in its design based on independent modules, suited to specific user needs.

The developer is thus guaranteed that, by using OROS, his applications will be able to take full advantage of the GCI400's advanced features:

- card management
- control of hardware peripherals, display, keyboard, buzzer, data memory, program memory, etc.

Return to Page Contents

GCR400: The Universal Smart Card Reader

Designed to offer maximum autonomy and ergonomic operation, the GCR400 incorporates all features required for desktop computing as well as transparent smart card reader functions:

- □ autonomous power supply (battery)
- □ compact 3,54 x 1,02 inches (90 x 80 x 26 mm)
- □ data read/write operations, etc.

See a photograph of the GCR400 Smart Card Reader (35K bytes)

The GCR400 is suited to all applications that require a smart card/computer interface:

- □ electrical card personalization
- □ testing
- □ data read/write operations, etc.

In our age of miniaturized portable systems, this compact autonomous reader responds to the increasingly widespread use of smart cards. The GCR400 is the size of a portable computer the reader is easily carried around.

It can also be hooked up to a desktop work-station, with several possible configurations:

- □ fixed to the microcomputer
- □ placed horizontally or vertically on the desk.

Return to Page Contents

GCR400-FD: The PC-Integrable Smart Card Reader

The GCR400-FD (GCR400- Floppy Disk) is a smart card reader designed to be intergrated into a PC-compatible microcomputer. With this reader, Gemplus offers a compact, user-friendly solution for desktop computer environments.

See a photo of the GCI400-FD (40K bytes)

The GCR400-FD is ready to be installed in a 3"1/2 floppy drive bay. This device includes the following components:

- □ a smart card reader, built around the GCI400
- □ an extension card that is installed in the PC.

Using the 5"1/4 adapter, the GCR400-FD can also be installed in drive bays corresponding to this larger format.

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

The GCR400-FD is used transparently, and is especially well suited for logicial access control applications.

Like the GCR400 this device offers all features found on coventional smart card readers.

Optional:

The GCR400-FD can be supplied with a Plug-In format security module. This module upgrades application security.

The GCR400-FD is thus particularly well suited to serve as a dedicated reader for computer security applications.

Return to Page Contents

Gemplus' hardware know-how

In addition to the production of smart cards, Gemplus is continually expanding its range of hardware and software products. The card readers and couplers are the result of Gemplus' electronic expertise and thus complete the global product offer : smart cards, readers, applications.

Gemplus' R & D laboratories have designed the GCI400 to be a modular, high-performance and multi-purpose device. This coupler has indeed become an essential building bolck in new smart card systems for all types of applications.

Gemplus' extensive experience in the design of smart card readers has led to the development of highly-specialized new readers, and PCMCIA-compatible card readers.

Gemplus also develops custom card readers for specific needs, such as the GCR550 for the German Healthcare card application.

New technologies associated with the smart card are constantly being developed by the R&D team. Gemplus aims to meet customer needs and play a leading role in the development of new smart card applications.

Return to Page Contents

GEMPLUS Return to Home Page

Last updated 5th April 1996

MOTOROLA

Site Search

68HC05 and 68HC08 Overview

Motorola's 68HC05 and 68HC08 8-bit microcontroller families consist of a variety of microcontroller designs to meet the requirements of a broad range of applications. It all started with the 68HC05C4, and Motorola's CSIC (Customer-Specified Integrated Circuits) approach to microcontroller design. Today, customers can select from 180 standard 68HC05 CSIC devices.

Building on the success of the 68HC05, the upward compatible, higher-performance 68HC08 Family enhances the CSIC design philosophy, incorporating a flexible, modular design and a library of proven peripherals - to achieve even faster design cycle times, enhanced manufacturing quality, and maximum cost-efficiency.

Both products are constantly expanding to offer one-chip solutions for applications which would otherwise require multiple devices. The devices are characterized by a high level of integration within each MCU and a rich choice of combinations of features with which to create derivatives.

Preview Products by Major Markets/Applications:

- General Purpose
- Automotive
- Consumer
- Telecommunications
- Computer
- Industrial

Need help understanding acronyms like SPI, OSD, or FZ?
View our acronym glossary.

68HC05 General Purpose Microcontrollers

68HC05 C-Family:
These flexible, general-purpose devices feature a wide variety of memory options capable of handling complex programs. On-chip Serial Communications Interface (SCI) provides asynchronous communications, with software-selectable baud rates from 75 Hz to 131 kHz. The high-speed, synchronous 4-wire serial system Serial Peripheral Interface (SPI) is ideal for driving off-chip displays and peripherals. The 68HC705C8A is Motorola's most popular One Time Programmable (OTP) microcontroller.

All C-family devices include a powerful 16-bit free-running programmable counter in conjunction with input capture and output compare functions for simultaneous input waveform measurement and output waveform generation. A watchdog timer guards against runaway software in noisy environments.

68HC05 J-Family:
This 20-pin family provides a low-cost, low pin count, 8-bit upgrade for existing 4-bit applications. It combines a powerful 68HC05 CPU with a flexible, 15-stage multifunction timer and real-time interrupt capability. The 68HC705J1A is Motorola's most cost effective One Time Programmable (OTP) microcontroller.

68HC05 K-Family:
Our lowest-cost family offers a 16-pin count and is appropriate for logic replacement.

68HC05 P-Family:
This family offers an extremely cost-competitive 28-lead family of microcontrollers with a variety of ROM sizes and special features such as Serial Input/Output Port (SIOP) to control display drivers and communicate with other peripherals. Other options include A/D input and on-chip EEPROM for non-volatile data storage. Low-voltage and high-speed versions are also available. The 68HC705P9 is Motorola's most popular One Time Programmable (OTP) microcontroller with an Analog to Digital Converter (ADC).

68HC08 XL-Family:
The flagship 68HC708XL36 OTP and 68HC08XL36 ROM versions are the first two devices in the 68HC08 family and are intended for general purpose uses.

Automotive

68HC05 B-Family:
68HC08 AB-Family:
EEPROM memory in these devices makes it possible to store information that must be retained after the power is removed. Applications include electric seat control (storage of seat positions) and audio systems (storage of radio stations). The B family has eight different versions from the popular 68HC05B6 to the new 68HC05B32.

68HC05 C- & D-Family:
These general-purpose microcontrollers are used for cruise control, ignition systems, and entertainment systems.

68HC05 J-, K-, and P-Family:
With their low pin count and low cost, these devices are ideal for automotive applications such as car alarms, power windows, keyless entry, and air bags.

68HC05 V- & X-Family:
68HC08 AS- & AZ-Family:
Both these groups contain integrated automotive multiplex interfaces that allow them to talk to other electronic modules within a vehicle. The V family adds an on-chip voltage regulator.

Computer

68HC05 BD-Family:
These MCUs are ideal for computer monitor applications. They include a horizontal and vertical sync processor as well as up to 16 channels of pulse-width modulation.

68HC05 C-Family:
These are general purpose devices for keyboard and monitor control.

68HC05 J-, P, & E-Family:
These low-cost, low pin count devices are appropriate for applications like a cordless PC mouse and trackball.

Consumer

68HC05 C- & D-Family:
The multiple communication lines (I/O ports, SCI and SPI) and free-running timer in this group of devices makes it possible to execute several tasks in parallel. These features are used in consumer products like CD players, automotive entertainment systems, and remote controls.

68HC05 J-, K-, & P-Family:
The free-running timer in these cost-effective microcontrollers allows multitasking in applications such as washing machines, oven controls, and remote controls.

68HC05 L-Family:
These low-power, small-footprint devices can drive large LCD displays, making them ideal for hand-held consumer products like portable CD players.

68HC08 LN-Family:
This 144 lead QFP device is targeted at applications that require large on-chip LCD displays, such as high-end cordless/corded telephones.

Industrial

68HC05 B-Family:
68HC08 AB-Family:
On-chip features include EEPROM; 8-channel, 8-bit A/D converter; and Pulse Length Modulated outputs. Typical industrial applications include Programmable Logic Controllers (PLC) and data acquisition systems.

68HC05 C- & D-Family:
These general-purpose devices can be used in applications such as process control systems where multiple I/O lines and LED outputs are required.

68HC05 J- and P-Family:
These devices are popular in low-cost industrial applications such as smoke detectors, security devices, thermostats, and furnace ignition systems.

68HC05 MC-Family:
This 28 pin device is optimized for low cost motor control applications with its on chip A/D converter and high speed PWMs.

68HC08 MP-Family:
This 64 pin device is targeted at motor control applications with on-chip A/D converters and a new 6 channel PWM module optimized for motor control applications.

68HC05 L-Family:
68HC08 LN-Family:

Multi-port controllers with LCD driver, 16-bit timer and watchdog timer on board. Excellent for display panels requiring tone output and low power consumption such as thermostats and alarms.

68HC05 X-Family:
68HC08 AZ-Family:
These devices have Controlled Area Network (CAN) controllers with 4k through 32k ROM for integrated messaging on factory automation, sensor, and switch applications.

Telecommunications

68HC05 B-Family:
68HC08 AB-Family:
These devices can store user-programmable telephone numbers in 256 bytes of non-volatile EEPROM memory. They can also interface with analog inputs like voltage by using the A/D module for measuring battery life in hand-held equipment. The D/A module can be used to control analog outputs such as telephone volume and line cards.

68HC05 C-Family:
This group of microcontrollers has proven useful as a general-purpose device for communications applications in phones and answering machines.

68HC05 E-Family:
Like the 68HC05 B-Family devices, E-Family devices are ideal for number storage and keyboard interrupt applications.

68HC05 F-Family:
These devices - except for the F5, which features an integrated DTMF receiver - include an on-chip Dual-Tone Multi-Frequency Generator (DTMG) for digital transmission and reception, as well as an LED drive for user information. These features make the F-Family suitable for a number of telecommunications applications, including auto dialing, number storage, and display control.

68HC05 J- & P-Family:
These low pin count, low-cost microcontrollers have a variety of telecommunications uses, with features ranging from EEPROM to multifunction timers.

68HC05 L-Family:
68HC08 LN-Family:
With its large LCD driving capability and low power consumption, this family is well-suited to applications in hand-held communication equipment. The on-chip tone generator and display functions can be used in pager systems to alert users to incoming messages.

Television & Video

68HC05 B-Family:
68HC08 AB-Family:
These devices are ideal for EEPROM storage, with 256 bytes of EEPROM to store TV or satellite channel frequencies and preset volume or brightness levels. Features include Analog-to-Digital (A/D) conversion and pulse-width modulation (PWM).

68HC05 C- & D-Family:

With up to 32k of user ROM, these devices can be used in the television and video market as general-purpose microcontrollers.

68HC05 CC-Family:
Evolved from the T-Family, CC-Family devices feature closed-caption Data Slicer (DSL) and enhanced On-Screen Display (OSD) features for decoding and displaying closed captions.

68HC05C0:
This device has no on-chip user ROM, but is capable of addressing up to 64k of external memory, making it ideal for applications that require large amounts of operating code, like televisions. The SCI+ module and 4 MHz bus speed allow interconnection with standard TV peripherals.

68HC05 K & RC-Family:
These devices are used in remote control applications.

68HC05 M-Family:
These devices have Vacuum Fluorescent Drive (VFD) capacity to drive high-voltage videocassette recorder displays.

68HC05 T-Family:
All T-Family devices have On Screen Display (OSD) modules that can overlay graphical images onto television screens. They also contain D/A converters that can drive analog outputs like volume control, and A/D converters that can be used to automatically adjust the fine tuning. Some members of the T-Family have I2C interfaces that can communicate with industry-standard TV peripherals.

Special Features

Low-Voltage Microcontrollers
The 68HC05 Family has been capable of 3.0 V operation since 1980 and includes some 2.2 V selections. Recently, Motorola announced several 68HC05 microcontrollers capable of 1.8 Vdc and 500 kHz operation. This new low-voltage capability affords a greater than threefold power savings over 3.0 V versions of the same chips, a significant design consideration for any portable electronic application. The new devices are collectively designated 68HCL05 and include the following versions: 68HCL05C4, C8, C12, J1A, K0, P1, and P4. They are designed to provide lower-power control technology to accommodate trends in portable applications toward compactness, lightweight design, and extended battery life.

Expanded Memory
The 68HC05C0 is an expandable 68HC05 microcontroller which does not have any on-chip user-programmable ROM. It has been designed to address up to 64k of external memory. As such, it is available off the shelf without mask charge or delay.

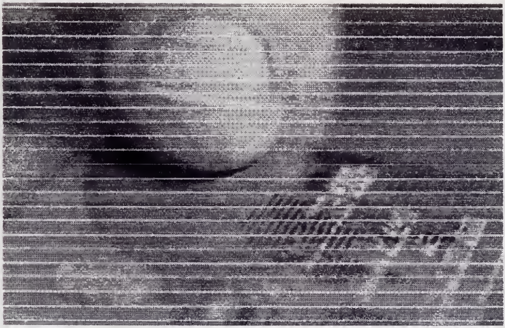
Security Features
The 68HC05SC11, SC21, SC24, SC27, and SC28 microcontrollers comprise a family of devices designed to be used in systems that require security. These devices have features that can enhance security by restricting access to the device-resident software and by allowing identification and tracking of each individual die. Most commonly delivered in die form for use in Smartcards for banking, cable and satellite television, and access control systems, they are also available in packaged form.

Combinational Technology
The 68HC705V8 is the first in a family of "system chips" from Motorola. A system chip integrates a variety of process technologies to reduce the number of electrical components and allow for smaller

designs, improved reliability, and less power consumption. The 68HC705V8 is the industry's first single chip multiplex module; it combines the HC05 core with an on-chip voltage regulator, J1850 multiplex bus with integral bus transceivers, A/D, EPROM, EEPROM, static RAM, timer, serial port, PWMs, COP, and low voltage inhibit.

Return to 68HC05 and 68HC08 Home Page
Go to What's New
Go to Technical Data Books/Appnotes
Go to Technical Support
Go to 68HC05 Selector Guides
Go to 68HC08 Selector Guide
Go to Development Systems

Last updated 9/10/96



Schlumberger
Measurement & Systems

Electricity Management

Gas Management

Water Management

Automatic Test Equipment

M & S Organization

Market & solutions

The universe of smart cards

Worldwide Presence

Welcome to Schlumberger

Electronic Transactions

The Schlumberger Electronic Transactions group offers a flexible set of smart card-based solutions for business for all kinds and sizes. This innovative offer, The Smart Village®, features smart cards, terminals, development tools and support for operators and developers around the world. Participating in The Smart Village® truly empowers you to leverage new convenience as lasting competitive advantage. Whether open or closed, public or private, an electronic transactions infrastructure will help your business to reach its full potential.

The Smart Village®

Visit The Smart Village®: the ideal integration of Smart Cards and related terminals, development tools and support.

Markets & solutions:

The extensive Schlumberger product range covers all the main smart card transaction fields, providing expertise and worldwide support for all your transaction needs: Telecom, Banking & Retail, Parking, Transportation, Petroleum Retail, Health Care, Automatic Vending.

Explore the Universe of Smart Cards! Inherent advantages, Where are they used?, Technology, Product range, Develop your own application.

Our difference:

- □ Truly global expertise in secured paperless and cashless transactions
- □ Specific organizations delivering state-of-the-art solutions dedicated to each market segment
- □ Local presence to meet local requirements and provide customer support
- □ Time-to-market development process to help our clients reach their potential

Electronic Transactions at a glance:

- □ 3300 people of 29 nationalities
- □ 35 facilities in 19 countries
- □ 9 research and development centers in America, Europe and Asia
- □ 120 millions smart cards delivered annually
- □ 500,000 + terminals in use in more than 60 countries

[illegible]

[illegible]

Schlumberger

| Top | Schlumberger Home |

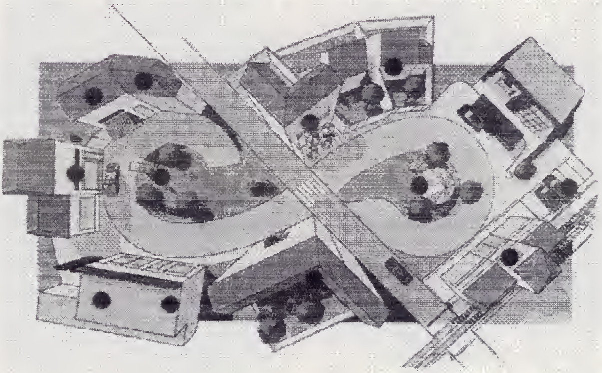
The Smart Village®

Schlumberger
Electronic
Transactions

A modular set of smart card-based solutions for public and private markets. The Smart Village®* leverages convenient transactions as competitive advantage for businesses and communities of every kind. The Smart Village®*; features smart cards, terminals, development tools and support for communities, operators and developers around the world. By joining the Smart Village®*, your products and services become more accessible to an ever-expanding customer base.

*Card-Based infrastructure for public and private communities of all sizes.

Click on areas of your choice to become a citizen of the Smart Village



Schlumberger

What's New | Search | Investor Relations | Oilfield | M & S | Recruiting | QHSE

irsupport@slb.com

| Top | Schlumberger Home|

MAIN

SEARCH

EUROPAY International

FAQ

Frequently Asked Questions

There's been much talk about security in cyberspace; is it safe to send credit card numbers over the Internet?

No, not in today's environment. If your credit card number is sent over the Internet without any security protections, the number could be intercepted and then used by fraudsters to make purchases against your account.

But can't they do that when I use my card in the physical world?

Yes, that's why it is always important to observe some basic **guidelines** when using your credit cards. The difference is that it is much easier to intercept information over the Internet without you knowing that it has even happened.

Doesn't using a secure communications channel like SSL solve the problem? Why do I need something else?

Security solutions like the Secure Sockets Layer only provide security from your browser to the merchant's server. Once your card information is read in the merchant's server, it is decrypted and visible again. If the merchant stores payment details on the server, then a criminal might be able to break in later and steal many card numbers.

The iKP solution that Europay is working on with IBM provides true multi-party security. Your payment details are encrypted to the merchant's bank. The details are not visible until the merchant's bank has received the payment request.

How is the bank's computer more secure than the merchant's computer.

The bank's computer that is connected to the Internet does not keep any payment details in an accessible form, and since it is a highly specialised system that only handles payment requests, it is easier to make it very secure. Many merchants operate their own systems in a fairly secure manner, but it is much more difficult to establish the overall security with a merchant's server than within the banks' systems.

What about smart cards?

In June 1994, Europay became the first international payment card organisation to commit to chip as the replacement technology for the magnetic stripe. Europay's Chip Business Case focussed on four key areas: Fraud Reduction, Telecommunications Cost Reduction, Credit Risk Management, and Value-Added Services such as its electronic purse product - "CLIP" launched at Europay's Third Members' Meeting held in Seville, Spain in June 1996.

Designed for making smaller value purchases not practical for credit and debit cards, the electronic purse will be an ideal way to pay for information and goods over the Internet.

Last Update: 26/08/96

MasterCard International

MasterCard Shapes the Future of Electronic Commerce

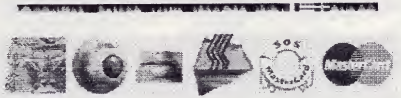
Today, you can purchase goods in many more places -- and in more ways -- than ever before. Gone are the days when you needed cash to buy goods and services. Now, you can shop whenever, wherever, however you want... on the Internet, from an airplane, sitting in traffic... from your telephone, ATM, PC and more.

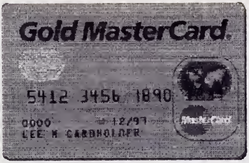
MasterCard International is at the center of these exciting new changes, leading the way in the expansion of commerce. And, we're committed to providing you with the most secure, most convenient way to purchase goods, and access and manage your money.

How does MasterCard International give you more options in how to pay, and where you can do business? One good example is the development of Chip cards, payment cards with an embedded microchip. EMV (Europay MasterCard Visa) specifications support the development of Chip card technologies, hardware and applications. This new technology will provide a stable, safe environment to use your MasterCard around the world. Another important development is commerce on the Internet. MasterCard has helped design a secure way (Secured Electronic Transactions, or SET) to use your bank card on the Internet, with new technologies and standards that make it easy -- and safe -- for you to purchase goods and information online.

Download Secure Electronic Transactions (SET) specifications

Download Chip Card Worldwide Transactions (EMV) specifications





EMV sets standards for global integration of Chip cards

What are Chip cards... and what can they do for today's consumers? Chip cards are the core of a new technology that provides a stable environment for worldwide electronic commerce. And for more than two years, MasterCard has worked with EuroPay and Visa to create global specifications for this important Chip card technology.

Known as EMV, these specifications offer a stable foundation for Chip cards as they financially bridge continental borders and telecommunications systems.

We are extremely pleased to provide you with EMV96, a three-book series of specifications addressing cards, terminals and applications.

This new release reflects comments received from the financial industry on Card Specifications Release 2.0 and on Terminal Specifications Release 1.0. This feedback has been carefully reviewed by our joint team, and most suggestions have been incorporated in these new releases. Plus, industry experts have reviewed the documents as well.

EMV 96 now supports applications that enable issuers and consumers to start using Chip cards and terminals-- with added security. Divided into three books, the EMV specifications include:

- **Card Specs** --a common basis regardless of application. Addresses electromechanical, commands, file and data structures, selecting applications and security. Plus secure messaging, post-issuance commands and Dynamic Data Authentication using the RSA algorithm.
- **Terminal Specs** --a common basis regardless of application. Provides details for a variety of different terminals.
- **Application Specs** --traditional payment transactions with the ability to add -- if jointly agreed -- additional applications, such as loyalty programs, etc.

You'll notice that stored value applications are not addressed in the application book. The EMV group realized that additional experience is needed with this new form of payment before common specifications are agreed to. However, they are addressed in the Card and Terminal specs, along with other products, regardless of how the application is implemented.

Chip card technology is a cornerstone for secure worldwide transactions. MasterCard is helping to lead the way... Shaping the Future of Electronic Commerce.

[illegible]

Download EMV specifications now:

EMV Specifications		
Card Specifications	**Terminal Specifications**	**Application Specifications**
Microsoft Word	Microsoft Word	Microsoft Word
PDF	PDF	PDF
PostScript	PostScript	PostScript

Get Acrobat You will need Adobe Acrobat to view PDF documents.
Use the Get Acrobat button for downloading the free Adobe Acrobat Reader.

[illegible]

FAQs

About Mondex

□ How does Mondex work?
□ What is a Mondex card?

Product Characteristics

□ Why has Mondex chosen a cash payment structure?
□ What about privacy?
□ What's the difference between Mondex and a cheque?

Social Issues

□ If Mondex replaces cash, won't that put poor people at a disadvantage?

Comparison with Competitors

□ What makes Mondex different?
□ What about competitors?

Mondex and Consumers

□ If my card is lost, or stolen, do I lose the money on it?
□ Can I take the card through Airport Security?
□ What happens if my card is damaged but still holds value?

Pricing

□ Will people be prepared to pay for Mondex?
□ What Mondex devices would I need to buy?

Mondex and Retailers

□ Why should retailers accept Mondex?

Security

□ How secure is Mondex?

Economic Issues

□ Will Mondex support the European Monetary Unit (EMU)?

Scheme Structure

□ How will the scheme be structured?

Mondex Suppliers

□ Which technology vendors are involved in the pilot for Swindon?
□ Are the manufacturers for Mondex restricted to those already commissioned?

Byte

□ What is the Byte trial?

UK Implementation

□ Who is implementing Mondex in the UK?
□ What is BT's involvement?
□ What are the UK launch plans?
□ Why was Swindon chosen as the pilot location?
□ Can people other than customers of NatWest and Midland banks get a Mondex card?

About Mondex

How does Mondex work?

Instead of carrying notes and coins, Mondex consumers will carry a Mondex Card, on which cash is stored electronically.

Because Mondex cash is electronic it can be transferred over a telephone line.

Mondex cardholders can load money onto their cards at a new generation of cash dispensers, payphones and homephones.

Mondex cardholders will be able to make payments wherever the Mondex sign is displayed. All Mondex payments are simply transfers of value, just like paying with ordinary cash. Shops and service providers have their own cards on which Mondex value is accumulated, which can be paid into their bank accounts as a bulk value at any time of the day or night via a Mondex telephone.

Mondex also enables person-to-person payments. Using a Mondex wallet, two cardholders can transfer cash between their cards. With a Mondex telephone, person-to-person payments can be made across the world.

Mondex cards can store up to five currencies electronically.

Back to FAQ Menu

What is a Mondex card?

The Mondex card is an integrated circuit (IC) card; a 'smart' card - a normal plastic card with a small microcomputer 'chip' embedded in it.

This microcomputer has been programmed to function as an 'electronic purse'

The electronic purse can be loaded with 'value', which is stored until it is used as payment for goods or services at retailers or service outlets that participate. The current balance on the card can be checked simply by inserting the card into a balance reader.

The electronic purse can also be locked using a personal code so that only the card's owner can use the value on it or check the transaction log.

Back to FAQ Menu

Product Characteristics

Why has Mondex chosen a cash payment structure?

Within the global payments market cash accounts for approximately 90 per cent of all transactions. Cash dominates the global payments market because it is the only product which delivers worldwide acceptance: instant and unaccounted transfer of value without a third party being involved.

For both retailers and consumers, cash is the only means of immediate, physical transfer of value. Other payment methods typically require some form of clearing and settlement - impossible for private individuals, impractical for small value payments and expensive for small retailers.

Mondex is an alternative to cash. It was developed to truly replicate the core features of cash and to be a real alternative to traditional notes and coins. Mondex has the potential for worldwide acceptance because value is transferred instantly and between individuals without involving a third party.

Individual Mondex transactions are not accounted through the banking system - there is no need for PIN or authorisation at the point of sale, and person-to-person payments can be made without the need for a third party.

Back to FAQ Menu

What about privacy?

In everyday use Mondex transactions are private, just like cash.

In addition to Mondex value ('cash'), cards also contain a 'purse narrative'. The transaction log on the customer's card records the narrative of the shop's card - thereby reminding the customer where they have used their card.

Only a cardholder will have access to the statement entries on their card which detail the most recent transactions. A cardholder will be able to lock their card and prevent unauthorised access.

However, if the card is lost, a unique 16-digit identity number stored on the chip, which will have been registered by a card-providing bank against the personal details of the customer, may be used in order to return the card to its rightful owner.

Back to FAQ Menu

What's the difference between Mondex and a cheque?

Mondex is cash.

Retailers will prefer the Mondex card because they receive the value instantly - there is no need to wait for a cheque to clear.

Payment will be faster than with a cheque - there is no need for writing out and bank card checking. So you can make small as well as large purchases with your Mondex card.

When you go shopping or travelling there will be a higher limit available for a transaction than with a cheque, up to £500 at the moment.

Back to FAQ Menu

Social Issues

If Mondex replaces cash, won't that put poor people at a disadvantage?

Mondex will be available to all sections of society, whether or not they are creditworthy.

Cash will remain important to certain sections of society and an important mechanism for spontaneous charitable donations.

But for events such as Live Aid many people might find it easier to send money down the telephone line using Mondex rather than to pledge money and then find a bank which is acting as a collecting agent the next day.

Back to FAQ Menu

Comparison with Competitors

What makes Mondex different?

Mondex is **open** and has no requirement for clearing - it is a payment system with the potential to be accepted everywhere. It has been developed as an alternative to traditional cash by allowing value to be received and transmitted between parties who are unrelated other than through their participation in the scheme, without the involvement of a third party.

Mondex has been designed to be a **global** payment system. International interoperability has been catered for by the adoption of standards, in the selection of the Mondex Brand and the employment of language-independent ergonomics. This means that it will be as easy to use a Mondex card in a shop in the UK as it will be to do so in Japan or India.

Mondex is *designed* to be **multicurrency**. It has been designed to operate in any participating currency and each purse is designed to carry up to five of the participating currencies at any one time.

Mondex has been designed to allow **person-to-person** payments, over a telephone line or via an electronic wallet device.

Back to FAQ Menu

What about competitors?

Given the current widespread use of cash, the market for products such as Mondex is huge and, given the huge cash market, there is room for more than one player in this market.

We believe that the success of Mondex will lead to competitive products being developed, but Mondex will be the first global alternative to cash on the market and will prove to be the standard for future competitive products.

From a technical point of view, as long as other products fall in line with relevant ISO standards, the global standard for Integrated Circuit cards, customers will be able to use competing products in a 'common' terminal at the retailer.

Back to FAQ Menu

Mondex and Consumers

If my card is lost, or stolen, do I lose the cash on it?

If you lose your card, or if it is stolen, the value is lost - just as it would be if you dropped a ten-pound note.

Mondex allows cardholders to lock their card, preventing other people from spending the cash on it.

This might enable banks to operate a return and reward system, and increase the chances of the return of cards to their rightful owners (where they can be identified); something that could never happen with a lost ten-pound, hundred-franc or thousand-peseta note.

Back to FAQ Menu

Can I take the card through Airport Security?

Yes. Mondex complies with ISO specifications in the area of card reliability, and with the harsher GSM specifications for protecting mobile telephones in everyday use. Mondex chips have been designed to withstand normal extremes of cold and heat, damp, X-rays or electrical interference.

Back to FAQ Menu

What happens if my card is damaged but still holds value?

If, for any reason, value is lost under normal environmental conditions, the cardholder can contact the issuing bank who will validate the claim and reimburse the value.

Back to FAQ Menu

Pricing

Will people be prepared to pay for Mondex?

Market research with over 5,500 consumers in eight countries indicates that people are prepared to pay for the significant advantages that Mondex offers.

Mondex is **convenient** - Mondex is easier to carry than cash. With Mondex you always pay the exact amount, without any need for change. Transactions using Mondex are faster than any other method. You can obtain electronic cash using Mondex at any time from an ATM or by telephone.

Mondex is **flexible** - Mondex is suitable for any value of transaction, unlike other payment methods, which may be appropriate only in certain situations (for example, credit cards and cheques may be seen as suitable only for larger payments). With Mondex you can pay in person or remotely using the telephone. No other form of payment, except cash, has the same ability as Mondex to make immediate person-to-person payment.

Mondex allows you **control** - With Mondex you can see how much money you have. You can spend only what you have and do not risk of incurring debt. With Mondex you can keep track of how much you have spent and where.

Mondex is **secure** - Mondex allows you to lock your 'electronic purse' with a personal code to prevent unauthorised use.

Back to FAQ Menu

What Mondex devices would I need to buy?

To use Mondex as a consumer you only *require* a Mondex card. It is anticipated that all cardholders will also want to have a balance reader. The balance reader will enable the cardholder to see the balance on their card at any time.

The holder of a Mondex card will be able to load the card with value at ATMs or using a public telephone and spend the value at participating retail outlets. Cardholders will also be able to lock and unlock the value on their cards.

Cardholders will be able to make person-to-person payments to a third party who has a Mondex wallet or a Mondex telephone.

Back to FAQ Menu

Mondex and Retailers

Why should retailers accept Mondex?

Mondex will bring many benefits to retailers:

- Mondex will improve efficiency and customer service, because there will be no need to give change or wait for authorisation/signatures at the point of sale - so transactions will be faster.
- Mondex will improve security and reduce risk of loss, because retailers will be able to transmit value to their bank at any time of the day or night as often as they wish. POS terminals can be set to 'receive only', so that Mondex value cannot be paid out of the purse in the terminal without a lock code being entered. This will reduce pilfering.
- Mondex avoids the cost associated with cash and cheque handling - reconciliation, custody and transportation.
- Mondex will improve control because more information about transactions and sales value can be retrieved more quickly. In addition, Mondex makes it easier for retailers to balance their tills.
- Mondex is guaranteed value and does not require any checking or verification, unlike paper money, which is threatened by the possibility of counterfeits.

Back to FAQ Menu

Security

How secure is Mondex?

IC cards offer a high level of protection against software attack and protection against physical attack or re-engineering. They also offer scope for considerable enhancement as technology advances.

Each time a Mondex card is used the chip generates a unique 'digital signature' which can be recognised by the other Mondex card involved in the transaction. This unique signature is the guarantee that the cards involved are genuine Mondex cards and that the transaction data is unmodified.

The security will be frequently changed so that fraudsters or hackers intending to target Mondex will find a fast-moving zig-zagging target that will make their efforts to break it unrewarding. By continually changing and increasing the complexity of the development program Mondex is designed to stay ahead of increasingly sophisticated criminals. The complexity of this security is so great that we believe it will not be economically viable for even highly organised crime to break it.

Back to FAQ Menu

Economic Issues

Will Mondex support the European Monetary Unit (EMU)?

Mondex has been designed to operate in any currency. This could include the (European Monetary Unit) EMU if it becomes legal tender.

Back to FAQ Menu

Scheme Structure

How will the scheme be structured?

A number of participants will be involved in the Mondex scheme.

Mondex International- will have an exclusive licence from NatWest Bank of the Mondex intellectual property rights (IPR) in order to develop the Mondex scheme and will licence participants to use the IPR and the Mondex Brand to exploit Mondex through a series of Franchise Agreements.

Franchisees - banks, or an entity owned and controlled by one or more bank, will have the right and obligation to manage, promote and exploit Mondex in its specified territory.

Manufacturers - manufacturers will be licensed by Mondex International to produce Mondex equipment for supply to any Mondex scheme participant or to third parties. Mondex equipment will be subject to type approval to ensure compatibility with Mondex specifications.

Merchants and other service providers - acceptors of Mondex electronic cash as payment for goods and services.

Back to FAQ Menu

Mondex Suppliers

Which technology vendors are involved in the pilot for Swindon?

Devices for the Mondex launch in the UK are initially being developed by:

- □ AT&T Global Information Solutions (formerly known as NCR) - cash machines
- □ British Telecommunications plc (BT) - residential telephones and payphones
- □ Dai Nippon Printing Co. Ltd/SPOM Japan Co. Ltd - cards
- □ De La Rue Fortronic - retailer terminals;
- □ General Information Systems Ltd. - electronic wallets
- □ Hitachi Ltd - a wide variety of devices and integrated circuits. Full details are available from the Hitachi Mondex Web site.
- □ Oki Electric Industry Company Ltd - electronic wallets
- □ Panasonic (Matsushita Electric Industrial/Matsushita Battery) - electronic wallets and personal balance readers

However, the list of potential device manufacturers is not restricted to those already commissioned.

The full range of organisations associated with Mondex is detailed in the Mondex File.

Bona fide manufacturers interested in the Mondex specifications may obtain information by applying to Mondex.

Back to FAQ Menu

Are the manufacturers for Mondex restricted to those already commissioned?

No.

In 1994 NatWest released the following specifications to manufacturers interested in producing Mondex devices.

- □ IFD (Interface Device) - **Purse Application Interface Specification** - This covers the interface between a Mondex card and any device offering Mondex functions. The specification defines the commands to which a card will respond and refers to the relevant international standards covering general communications to and from IC cards.
- □ **Introduction to Mondex Purse Operation** - This is a companion document to the above. It provides an overview of the Mondex card and its interface with a Mondex device.
- □ **The Mondex Brand Manual** - This document defines the permissible implementations of the Mondex brand.

Other specifications will cover the communications between two interface devices, the user-interface standards designed to ensure user-friendly product design and the card specification.

Manufacturers interested in Mondex specifications should contact Mondex directly.

Back to FAQ Menu

Byte

What is the Byte trial?

The Byte trial was the first test of Mondex in a live environment.

One of NatWest's major computer centres, Goodmans Fields in London, was chosen as the test environment.

Approximately 6,000 NatWest staff were issued with cards to be used in the centre's restaurants, coffee bars and shop - in total, twelve points of sale. The NatWest branch in the same building, which operates three ATMs and several counter terminals to allow staff to load their cards, also participated in the Byte trial.

The trial has been very useful to NatWest, both in measuring customer reactions and in testing the reliability of the technology. By the end of 1994 more than 1 million purchases had been successfully been made using the technology.

Market research undertaken in Goodmans Fields has shown that people who used the card found it more convenient and quicker to use than cash.

And key elements that people wanted added to Byte have been incorporated into Mondex, including:

- □ The facility to lock the card.
- □ Provision of a simple portable device to enable them to read the balance on the card.

Back to FAQ Menu

UK Implementation

Who is implementing Mondex in the UK?

NatWest has joined forces with Midland Bank to purchase the Mondex franchise in the UK.

The two banks have established a joint venture company, called **Mondex UK Limited.**

Together with BT, the banks will be responsible for the pilot being undertaken in Swindon and eventual national rollout of Mondex.

Back to FAQ Menu

What is BT's involvement?

BT is developing and supplying home telephones, public payphones and retailer phones that provide Mondex functionality for the Swindon pilot.

Back to FAQ Menu

What are the UK launch plans?

3 July 1995: MONDEX LAUNCHED - READ ALL ABOUT IT

A high-street newspaper vendor in the UK made history today when he officially became the first person to exchange goods for electronic cash.

Don Stanley, 72, parted with a 28p newspaper in return for 'cash' stored in the microchip in his customer's Mondex card.

The simple transaction marked day one of a pilot in Swindon, Wiltshire, the first step in the introduction of a global alternative to cash.

From now on, Swindon's shoppers will be able to pay for goods and services at outlets - from corner shops to department stores - without having to worry about breaking into £20 notes or fiddling with small change.

Mondex has been developed jointly by the NatWest and Midland Banks and BT, and is being heralded as one of the biggest breakthroughs in money since the introduction of cash machines in the 1970s.

Mondex is based on the electronic storage of money on a plastic smart card. It can be used to pay for

goods and services in the same way as notes and coins, and the 'cash' can be transferred from one card to another, or to and from a bank account, using a range of Mondex devices or compatible BT phones.

Unlike transactions using credit or debit cards, Mondex transactions do not involve authorisation or signatures and there is no chance of incurring debt because users can spend only what is available on their card.

The Swindon pilot is set to last up to two years and is expected to involve up to 40,000 consumers and 1000 retailers.

Mondex UK Chairman, **Tony Surridge**, said:

> "We're updating a form of payment which has been around for thousands of years. And whilst Mondex is essentially the same as cash, we've been able to add in a few important improvements - such as being able to send or receive money down a phone line."

Ken Howes, Head of Group Card Development at Midland Bank, said:

> "Although we expect the Swindon pilot to herald a 'less-cash' rather than a 'cashless' society, we believe that people will find Mondex extremely convenient and will use it as they use cash now."

Geoff Finch, BT's director of Card Services, added:

> "The ability to transfer cash over the telephone is a revolutionary development in the history of money and telecommunications."

Swindon was chosen for the pilot as it has a population profile that is representative of the UK and has a wide retail and commercial base.

Beyond the pilot, Mondex will be extended across the UK and internationally. The Bank of Scotland has already agreed to participate in the scheme on a national level, The Hongkong and Shanghai Banking Corporation Limited has purchased the rights to Mondex in the Far East, the Royal Bank of Canada and Canadian Imperial Bank of Commerce have purchased the rights to Mondex in Canada, and ten leading banks in Australia and New Zealand have purchased the franchises for Australia and New Zealand.

Back to FAQ Menu

Why was Swindon chosen as the pilot location?

Swindon (a large town in South West England, 70 miles from London) is playing a leading role in the introduction of Mondex in the world.

The town, of some 190,000 citizens, is recognised as one of the UK's most progressive commercial environments - and has successfully attracted a wide range of major companies including Intel, Rover and British Aerospace.

Shoppers in Swindon can choose from over 700 participating retailers, including the majority of the High Street Names.

For market research purposes the demographic profile of Swindon consumers is very similar to the UK

national average.

Back to FAQ Menu

Can people other than customers of NatWest and Midland banks get a Mondex card?

Yes. Both Midland and NatWest are able to offer the Mondex service to customers of other banks.

The early emphasis is to recruit cardholders from amongst their own customer bases as a start, including the offering the service to members of customers' immediate families, even though they may not hold a direct account relationship.

Back to FAQ Menu

HOME

VERISIGN, INC.

About VeriSign, Inc.

"Putting Trust Into Electronic Commerce"

VeriSign, Inc. is the leading provider of digital authentication services and products for electronic commerce and other forms of secure communications.

> VeriSign's services and products are divided into three lines of business: Digital ID Services, Private-Label Certificate Services, and Certificate Management Products.

VeriSign, founded in 1995 as a spin-off of RSA Data Security, is working with its investors including Ameritech and Visa International, and partners such as Netscape, Open Market, and IBM to open the digital marketplace to all consumers. VeriSign's goal is to provide consumers, merchants and corporations with the confidence necessary to conduct electronic commerce worldwide.

Digital IDs (also known as digital certificates) play a key role in establishing confidence that electronic transactions are secure and trusted. A Digital ID binds a person's or company's identity to a digital key which can be used to conduct secure communications or transactions.

This binding is accomplished through a strict assurance process conducted by a trusted third party which also electronically signs the Digital ID so that parties accepting it in a transaction have confidence in it's origin. The Digital ID can then be attached to electronic transactions and communications as the critical authentication component.

As the fundamental shift to electronic commerce accelerates, Digital IDs and other types of digital certificates will play a vital role in authenticating and securing electronic transactions and communications.

###

SPRYNET

Member Support

- Join SPRYNET
- Online Support
- Customer Care

Resources

- Web Guide
- Software Central
- Personal Services
- Business Services
- Reference Desk

Community

- Personal Home Pages
- Chat
- Forums

Search

- Search SPRYNET
- Search the Internet
- SPRYNET Site Map

Home

Press *Releases*

CompuServe Ships SPRY SafetyWEB Server for Windows NT

Low Price and Competitive Features Makes SPRY SafetyWEB Server Best on the Market

BELLEVUE, WA, March 19,1996 - CompuServe Incorporated's Internet Division announced today the immediate availability *SPRY SafetyWEB Server*, one of the industry's highest performing and best-valued commerce and publishing Web servers on the market. *SPRY SafetyWEB Server* is available for the Windows NT platform and supports Secure Sockets Layer (SSL) transactions, Virtual Server multiple IP addresses and includes the Architext Excite search engine, HoTMetaL PRO HTML authoring tool from SoftQuad Inc., and *SPRY Internet Office*. *SPRY SafetyWEB Server* is priced at $895.

"I'm especially impressed with the *SPRY SafetyWEB Server's* ACL security management and the straightforward tools offered for connection to SQL databases via ODBC," said Tony Varela, system administrator for the Washington state Department of Health, Information Services. The Integrated Open Database Connectivity (ODBC) integration allows real-time access to corporate data in a wide variety of databases. It also enables logging of accesses to the Web site to an ODBC database, allowing easy access from other ODBC clients such as Excel, Acess and Visual FoxPro.

"The Windows NT Web server market is growing quickly," said Tim Gelinas, vice president of World Wide Products for CompuServe's Internet Division, "and since *SPRY SafetyWEB Server* was written specifically for Windows NT, it gives customers a total secure Windows NT server solution at about half the cost of any competing product."

Unique SPRY SafetyWEB Server Feature For Windows NT

Windows NT is a strategic platform for CompuServe. CompuServe developers have been working with Windows NT for some time to parley some of the Information Services onto the Internet, and *SPRY SafetyWEB Server's* high performance and full functionality is a result of CompuServe's Windows NT expertise. *SPRY SafetyWEB Server* was recently awarded Microsoft's Backoffice certification which sanctions it fully compliant to true Windows NT standards.

- □ **Written for NT 3.51** and therefore is one of the most stable servers on the market for processing large volumes of data;
- □ **Remote Administration** allows webmasters to administer their site remotely via Windows 95 or Windows NT and gives complete file security privileges.

Enhanced Features Of SPRY SafetyWEB Server

SPRY SafetyWEB Server includes many important and powerful features such as:

- □ **Open Database Connectivity** (ODBC) that allows developers to directly query other ODBC compliant databases such as ACCESS, SQL Server, Paradox, Oracle and Sybase;
- □ **Proxy server** support to allow internal clients to traverse firewalls, as well as improving caching performance;
- □ **Digital Certificates** by the digital certification authority Verisign. For high performance scenarios;
- □ **Binary Gateway Interface** (BGI), Windows DLL can be called for database queries forms processing;
- □ **"Keep Alive"** support is another performance enhancement included that keeps the client/server connection;
- □ **CGI Scripts** brings power to forms processing and server extensibility.

Pricing and Availability

SPRY SafetyWEB Server is available for Windows NT operating systems. Pricing for *SPRY SafetyWEB Server* is $895(U.S.). A free copy of CompuServe's Internet client software *SPRY Internet Office* is also included. The non-secure server, called *SPRY WEB Server*, is now available for the list price of $245 (U.S.).

About CompuServe

CompuServe is an H&R Block (NYSE:HRB) company. Founded in 1955, H&R Block is a diversified services company and the world's leader in tax preparation and online information services. H&R Block Tax Services handled almost one in every seven returns with the Internal Revenue Service in 1995, serving 17.1 million taxpayers in more than 9,500 offices worldwide. CompuServe operates the most comprehensive online network in the world, providing services to more than 950 corporate accounts and more than 4.7 million users in 147 countries.

# # #

TIS Research

Cryptographic Technologies

TIS Worldwide Survey of Cryptographic Products

DESCRIPTION:
In order to determine how widespread cryptography is in the world, Trusted Information Systems (TIS) has been conducting a survey of products employing cryptography both within and outside the U.S. While some amount of information about specific products here and there has been available, no one has previously assembled a comprehensive database with, where possible, verification of product availability. Originally commissioned by the Software Publisher's Association (SPA) in May 1993 and conducted in cooperation with Dr. Lance Hoffman of the George Washington University, an ongoing survey for over three years. Information about cryptographic products continues to flow in on a daily baisis. We are releasing summary information on a periodic basis. The summary statistics as of June 1996 are reported below.

We have now identified 1262 products worldwide, and we're continuing to learn about new products, both domestic and foreign. We've also obtained numerous products from abroad and are examining these products to assess their functionality and security. The survey results show that cryptography is indeed widespread throughout the world. Export controls outside of the U.S. appear to be less restrictive. The quality of foreign products seems to be comparable to that of U.S. products. Given U.S. export restrictions, foreign customers who need cryptographic-based security for their unclassified but sensitive information now can turn to foreign rather than U.S. sources to fulfill that need. As a result, U.S. Government restrictions may be succeeding only in crippling a vital American industry's exporting ability!

CRYPTO SURVEY RESULTS:

Worldwide Availability of Cryptographic Products (as of June 1996)

FOREIGN PRODUCTS: We identified 532 foreign products from 28 countries:

```
Argentina      Australia      Austria
Belgium        Canada         Czech Rep.
Denmark        Finland        France
Germany        Hong Kong      India
Iran           Ireland        Israel
Italy          Japan          Mexico
Netherlands    New Zealand    Norway
Poland         Russia         South Africa
Spain          Sweden         Switzerland
UK
```

Of these, 217 employ DES, 92 in software programs and kits produced in the following countries:

Australia	5	Austria	1
Belgium	1	Canada	9
Denmark	5	Finland	3
Germany	17	Ireland	4

Israel	9	Italy	2
Japan	1	Netherlands	4
Poland	1	Russia	5
South Africa	4	Sweden	6
Switzerland	1	UK	14

Some foreign companies have distributors throughout the world, including in the U.S. One U.K. company has distributors in at least 13 countries, and one German company has distributors in 14 countries.

DOMESTIC PRODUCTS: We identified 730 domestic products, 349 with DES.

TOTAL PRODUCTS: Worldwide total of 1262 products produced and distributed by 816 companies (428 foreign, 388 domestic) in at least 68 countries.

SOURCES OF INFORMATION: To provide a definitive assessment of the manufacture and distribution of cryptographic products throughout the world, the survey makes use of numerous sources of information: computer security product guides, including Datapro reports, Elsevier PC Security Guide, Computer Security Institute (CSI) Computer Security Products Buyer's Guide, and INFOSecurity News Buyer's Guide; various trade press and journal articles; product literature; Internet electronic mailing lists and news groups; on-line computer hardware and software databases; the web; and foreign embassies and trade associations.

CONFIRMATION OF PRODUCTS: Information about cryptographic products is collected into a comprehensive database, with, where possible, verification of product availability through direct inquiries of product manufacturers and distributors.

TYPES OF PRODUCTS: The survey includes many types of cryptographic-based security products:

- □ hardware, firmware, software, or combinations thereof;
- □ general-purpose products (e.g., word processors, spreadsheets, telephones, or modems), as well as explicit cryptographic products (e.g., a PC file encryption utility);
- □ commercial mass-market products, as well as shareware and other products freely available via dial-up BBS connections or over the Internet via anonymous FTP or the Web;
- □ products providing confidentiality, integrity, and/or authentication service using cryptographic mechanisms.

OBTAINING FOREIGN PRODUCTS: We have obtained a number of products, focusing on software products employing the Data Encryption Standard (DES). The products were purchased via routine channels, either directly from the foreign manufacturer, or from a U.S. distributor. The products were shipped to us within a few days and in several cases, overnight. Implementations of DES, RSA, and IDEA were obtained freely over the Internet from sites throughout the world.

ANALYSIS OF SOFTWARE PRODUCTS: We have examined a number of domestic and foreign software products, looking at both the functionality and security characteristics of these products. While it is difficult to directly compare different products, we have developed a cryptographic security profile that we apply to products. The profile looks at numerous

characteristics of the products: basic program operation; cryptographic key entry, storage, verification, and recovery; cryptographic modes of operation, use of IVs and padding techniques; file headers; file zeroization; and the implementation of the cryptographic algorithm.

ADDITIONAL INFORMATION: To obtain further information on the TIS worldwide survey of cryptographic products, or to provide any information you may have about cryptographic products, visit the crypto survey Web page at http://www.tis.com/crypto/survey.html, or contact David Balenson at 301-854-5358 or by sending email to <balenson@tis.com> via the Internet.

Domestic Products | Foreign Products | Crypto Solutions

7/22/96

Research Products & Services Home Search

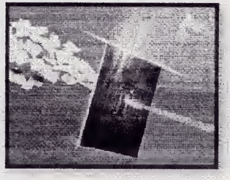
tis

Directory | Copyright Info | webmaster@tis.com

CKE

Overview

Commercial Key Escrow System
The path to global information security



We are living in the Information Revolution, the third great revolution of humanity. The Information Revolution succeeds the Agricultural Revolution and the Industrial Revolution and, like the two that have gone before, is accelerating at a pace that has not been experienced before on this planet. A dramatic alteration is taking place in the way information is transmitted and exchanged. The traditional face-to-face, paper-based system we have been using for the last thousand years or so is giving way to a new, faceless electronic commerce system that is rapidly proliferating on a worldwide basis.

Information Security Problems in Commerce

We are currently caught between paper-based authentication, privacy, authorization, and record-keeping systems, and electronic versions that are replacing them. This middle ground is painful. The paper-based systems still dominate, but they are falling prey to advances in counterfeiting technologies at an alarming rate. As an example, consider the driver's license-the preeminent paper-based personal authenticator. In Northern California, a counterfeit California driver's license can be bought on the streets for $90, and that includes entering the data in the Department of Motor Vehicles' computer!

But as the Information Revolution progresses, more and more paper-based systems are being replaced by electronic means. Examples include paying for groceries at the supermarket with our ATM cards, keeping our check registers on-line with Quicken, sending e-mail to our business associates, and browsing the World Wide Web to get configuration and dealer cost information needed to negotiate effectively with auto dealers. Unfortunately, the very thing that attracts us to electronic commerce-the ease of manipulating information-also works for an attacker in gaining access to critical information and using that information to damage the legitimate participants. Examples of electronic break-ins abound in daily life, and many people are wondering if electronic commerce is something to look forward to, or something to fear...

NEXT Cryptography: The Security Solution . . .

CKE Products & Services Research Home Search

tis

Directory | Copyright Info | webmaster@tis.com

THE SSL PROTOCOL

If you have questions about this specification or would like to send us your comments, please send email to ssl-talk@netscape.com. You can subscribe to this mailing list by sending email to ssl-talk-request@netscape.com and putting the word *subscribe* into the subject line or the body of the message.

The latest version of the SSL protocol has been submitted to the IETF and is available as an Internet Draft. Netscape is actively pursuing the standardization of SSL within the framework of the IETF standards process and is also working with industry consortium groups to ensure that open and interoperable security standards exist now and in the future. You can participate in the IETF effort by subscribing to the IETF mailing list: send email to ietf-tls-request@w3.org with *subscribe* in the subject. If you would like to send comments directly to Netscape during this process, please send email to standards@netscape.com. We review all comments we receive, but unfortunately we cannot provide individual responses.

Netscape has developed an SSL reference implementation of the Version 2.0 specification called SSLRef. You can apply to download SSLRef 2.0 for noncommercial use or, if you are interested in commercially licensing this reference implementation, please send email to ssl@netscape.com. The license restrictions for this reference implementation have no impact on anyone's ability to freely implement the SSL protocol purely from the SSL specification.

SSL VERSION 3.0, DATED MARCH 1996

Version 3.0 of the Secure Sockets Layer (*SSL V3.0*) is described in the specification document. SSL V3.0 is a security protocol that prevents eavesdropping, tampering, or message forgery over the Internet.

This version of the specification is dated March, 1996 and supersedes the December 1995 version. We thank everyone who participated in the open and valuable design discussions.

Netscape expects to ship products that conform to the March specification. Please note that Netscape server products with SSL V3.0 support both SSL 2.0 and SSL 3.0 protocols (SSL 3.0 was designed to allow this for transition purposes). SSL 2.0 has a limited lifetime.

NETSCAPE HOME | DOWNLOAD SOFTWARE | CUSTOMER SERVICE | TECHNICAL SUPPORT | SEARCH & CONTENTS | WEB SITE ADVERTISING

Corporate Sales: 415/937-2555; Personal Sales: 415/937-3777; Federal Sales: 415/937-3678
If you have any questions, please visit Customer Service.

ASSISTANCE

NETSCAPE DATA SECURITY

AN OVERVIEW OF IMPLEMENTATIONS AND PLANS FROM NETSCAPE COMMUNICATIONS

The following topics are discussed in this document (simply click on any subject area to jump to that section):

Please send us any comments or questions.

SECURE SOCKETS LAYER (SSL)

Netscape Communications has designed and specified a protocol for providing data security layered between application protocols (such as HTTP, Telnet, NNTP, or FTP) and TCP/IP. This security protocol, called Secure Sockets Layer (SSL), provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

SSL is an open, nonproprietary protocol. SSL has been submitted to the W3C working group on security for consideration as a standard security approach for World Wide Web browsers and servers on the Internet. We are working with the W3C and W3C members (including EIT) on developing and standardizing common, robust security mechanisms and protocols for the Internet. We will fully support such mechanisms and protocols as they become standardized.

You can apply to download SSLRef 2.0 for noncommercial use or, if you are interested in commercially licensing this reference implementation, please send email to ssl-talk@netscape.com. We will respond with license terms within three business days. The license restrictions for this reference implementation have no impact on implementation of the SSL protocol from the SSL specification. If you have technical questions about SSL and SSLRef, please send email to ssl-talk@netscape.com.

NETSCAPE NAVIGATOR

All versions of Netscape Navigator browser (beginning with 0.93 for Windows, Mac, and Unix variants) have integrated support for SSL. This support is implemented as follows:

□ Netscape Navigator supports a new URL access method, "https", for connecting to HTTP servers using SSL. SSL is designed to layer beneath application protocols such as HTTP, SMTP, Telnet,

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

FTP, Gopher, and NNTP. SSL is layered above the connection protocol TCP/IP.

- "https" is a unique protocol that is simply SSL underneath HTTP. You need to use "https://" for HTTP URLs with SSL, whereas you continue to use "http://" for HTTP URLs without SSL. The default "https" port number is 443, as assigned by the Internet Assigned Numbers Authority.
- Netscape Navigator is approved for export by the United States Government. The license states: "none of the Software or underlying information or technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident of) Cuba, Haiti, Iraq, Libya, Yugoslavia, North Korea, Iran, or Syria or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders." However, in general, the software can be freely used outside the United States.
- Because of export restrictions, Netscape Navigator is limited to a 40-bit key size for the RC4 stream encryption algorithm (the encryption algorithm used by Netscape Navigator's implementation of SSL). A message encrypted with 40-bit RC4 will take on average 64 MIPS-years to break (a 64-MIPS computer will need a year of dedicated processor time to break the message's encryption). This is not military-grade security, but the effort required to break any given "https" data exchange is definitely nontrivial.
- Netscape Navigator supports the standard X.509 cryptographic certificate format within SSL. Currently, Netscape only supports use of server certificates; clients may not (yet) have certificates.

Here's a brief overview of Netscape Navigator's graphical user interface (GUI) for security. This GUI is still evolving. Please send us comments concerning the interface.

- By default, a "security colorbar" appears at the top of each the Netscape Navigator window, right above the scrolling document area. If the colorbar is gray, the current document is not secure (that is, it was not transferred under cover of encryption); if the colorbar is blue, the current document is secure (that is, it was transferred under cover of encryption). The security colorbar does not indicate whether you can completely trust the document and its contents; it merely shows you at a glance whether the document was retrieved using encryption or not. The "Show Security Colorbar" option in the "Options" menu lets you turn the security colorbar on and off.
- An icon in the bottom left corner of each Netscape Navigator window indicates the exact same thing as the security colorbar. If the icon shows a broken doorkey over a light gray background, the current document is not secure. If the icon shows an intact doorkey over a dark blue background, the current document is secure.
- The "Document Information" entry in the "File" menu pops up a dialog box that contains more info about the state of the current document. The dialog box tells you the level of encryption that was used to transfer the document (as noted above, currently only export-grade, 40-bit RC4, encryption is supported). The dialog box also tells you who the remote server is by displaying the relevant fields from the server's certificate.
- Various informative dialog boxes are displayed in situations where you are entering a secure space, leaving a secure space, submitting a form insecurely, and viewing a secure document that contains insecure inlined images. You can disable the display of these dialog boxes after they first appear or via Netscape Navigator's Preferences dialog.

Netscape Commerce Server

NETSCAPE COMMERCE SERVER

Netscape Commerce Server (a commercial product, currently in wide 1.0 release) implements server-side support for HTTP over SSL, including support for acquiring a server certificate and communicating securely with SSL-enabled browsers like Netscape Navigator. Netscape Commerce Server provides additional functionality to make it easy for you to establish a security-enabled online presence on the Internet or on your corporate TCP/IP network. Features include easy configurability and maintenance, high levels of performance, full documentation, and technical support from Netscape Communications.

We will be producing U.S.-only versions of both Netscape Navigator and Netscape Commerce Server with high-level security support, including 128-bit RC4. We may distribute the U.S.-only version of Netscape Navigator over the Internet (depending on whether we determine it's safe for us to do so, given U.S. export laws).

Contact sales2@netscape.com for information on buying the export-grade and U.S.-only versions of Netscape Navigator and Netscape Commerce Server.

TECHNICAL DETAILS

Some information about SSL and our current implementations that may not be immediately obvious:

- SSL provides a security "handshake" that is used to initiate the TCP/IP connection. This handshake results in the client and server agreeing on the level of security they will use, and fulfills any authentication requirements for the connection. Thereafter, SSL's only role is to encrypt and decrypt the bytestream of the application protocol being used (for example, HTTP, NNTP, or Telnet). This means that all the information in both the HTTP request and the HTTP response are fully encrypted, including the URL the client is requesting, any submitted form contents (including things like credit card numbers), any HTTP access authorization information (usernames and passwords), and all the data returned from the server to the client.

- Netscape Navigator includes embedded Certificate Authority (CA) keys for certain CAs, including our test CAs. As new CAs come online, we will embed their keys as well. These embedded keys allow Netscape Navigator to verify the legitimacy of arbitrary servers. See the Document Information dialog to inspect both the identity of a given server as well as the identity of the CA that issued the server its certificate. SSL requires servers to have certificates issued by a Certificate Authority; Netscape Commerce Server includes a mechanism to easily acquire such a certificate.

- Currently, Netscape Navigator does not include support for NNTP over SSL or application protocols other than HTTP; however, such support will be available soon.

- Because HTTP+SSL (or "https") and HTTP are different protocols and typically reside on different ports (443 and 80, respectively), the same server system can run both secure and insecure HTTP servers simultaneously. This means you can provide some information to all users using no security, and other information only securely, if you so choose. For instance, your "storefront" and merchandise catalog could be insecure, and your ordering and payment documents and forms could be secure.

- Browsers that do not implement support for HTTP over SSL will naturally not be able to access "https" URLs. One of the reasons we are using a different URL access method ("https" instead of just "http") is so non-SSL browsers will gracefully refuse to allow insecure submission of forms that

expect to be submitted securely. That is, if a document served by a normal HTTP server contains a fill-out form that allows a user to enter his or her credit card number, and that form's submission action is an "https" URL (because the document's author expects the form to be submitted securely), a non-SSL browser will not even try to submit the form (typically giving a "cannot submit" error message instead). Were a separate URL access method not being used, the browser would try to submit the form, passing the credit card number over the net in the clear, and the submission would fail anyway.

THE RELATIONSHIP BETWEEN SSL AND SHTTP

SHTTP is a security-enhanced variant of HTTP proposed by EIT. SSL and SHTTP have different motivations: SSL layers security beneath application protocols like HTTP, NNTP, and Telnet, whereas SHTTP adds message-based security (drawing on the approaches and philosophies of the PEM and MIME efforts) to HTTP specifically. SSL and SHTTP are not mutually exclusive; rather, they can easily co-exist in a complementary fashion by layering SHTTP on top of SSL.

We will support NNTP over SSL (for secure NNTP news reading and posting) in our products soon. Most likely, we will support other application-level protocols (such as Telnet) over SSL as well.

We're considering support of SHTTP. (Note that SHTTP has not yet been blessed by any standards body, issued as an Internet RFC, or finalized as a protocol spec. Like SSL, it is still evolving and is a proposal to the W3C working group on security). SHTTP provides capabilities SSL does not, as SSL provides capabilities SHTTP does not. We are actively talking to and working with EIT and others, both under the W3C umbrella and separately, to evolve standard security approaches for the Internet.

We wish to emphasize our full support for open standards, open protocols, and interoperability. We do not advocate proprietary security solutions. We believe the attractiveness and viability of our products are enhanced in a cooperative environment.

NETSCAPE HOME | DOWNLOAD SOFTWARE | CUSTOMER SERVICE | TECHNICAL SUPPORT | SEARCH & CONTENTS | WEB SITE ADVERTISING

Corporate Sales: 415/937-2555; Personal Sales: 415/937-3777; Federal Sales: 415/937-3678
If you have any questions, please visit Customer Service.

NORTEL

Entrust

June 5, 1996

Contact:

Laura Teder
Nortel
214-684-8721
laura_teder@nt.com

Nortel Provides Data Security Technology to PayPro Network

Nortel announced today that Internet Payment Processing Inc. (IPPI), has selected Entrust, Nortel's data security software to provide security for Internet Banking. Nortel is helping IPPI meet the banking industry's strict security standards as they launch the PayPro Network.

The Pay Pro Network will provide an interactive, multimedia on-line banking and shopping environment, called CONSUL, which will offer consumers the full range of financial services they now enjoy through automated teller machines and Interac. In addition, CONSUL is expected to provide a range of consumer products and services over time.

"Customer confidence is dependent upon strong security when it comes to doing business via the Internet," said Brad Ross, director of business development, Nortel Secure Networks.

Entrust 2.0 is the only scalable security product available today that provides a public-key infrastructure for tens of thousands of users. Entrust's encryption, digital signature and key management technology is integrated with a number of leading client/server applications such as: OpenMail from Hewlett-Packard, FormFlow from Symantec Delrina Group and many others.

"The PayPro Network will be the first complete payment system for credit, debit and stored value cards over the Internet," said Gary Bartholomew, president of Internet Payment Processing Inc. "Our relationship with Nortel is driven by our needs for uncompromising security, global capability and field proven products."

In addition to Nortel, other companies contributing to the PayPro Network project are Digital Equipment Canada Limited, ACC Tele Enterprise Inc., Fleximation Systems Inc., International Verifact Inc. and Chrysalis ITS Inc. The network is scheduled for field testing this fall, and will be launched nationally in the spring of 1997.

Nortel is dedicated to ensuring the privacy and authenticity of data communications for enterprises. With 15 years of experience developing solutions and systems for secure communications, Nortel has built a team of world-leading experts in cryptography, security architecture and international standards. Nortel also offers Rapport, an Internet solutions portfolio, designed to make the public Internet more reliable, more secure and more profitable for everyone.

Nortel Home Page | Entrust Home Page | entrust@entrust.com

Nortel Home Page Entrust Home Page Comments?

Company Profile

Atalla: The leader in hardware-based transaction security

What the Business Is

Founded in 1972 by Dr. John Atalla, and acquired by Tandem Computers Incorporated in 1987, the firm pioneered hardware-based security for the financial and retail businesses and holds numerous patents in security, electronic banking and security chip technology. Atalla manufactures products for several markets: bank branch automation, retail point-of-sale, financial network security and Internet security. The products can be categorized as follows:

- □ Network security processors and modules
- □ Secure enrollment solutions
- □ Point-of-entry devices
- □ Cryptographic security management software

A brief description of these product categories follows.

Network Security Processors and Modules

Atalla network security processors (NSP) and modules are physically and logically secure cryptographic devices that provide maximum privacy, integrity, and performance in networks. Their hardware-based design eliminates the security risk inherent in software-based approaches. Atalla NSPs and modules perform a wide range of functions, including PIN processing, message authentication, encryption, decryption, and key management. They support many industry standards used worldwide.

A recent addition to the NSP family provides secure transaction processing over the Internet. The WebSafe Internet Security Processor supports both public key (RSA) and DES cryptographic technologies into a single hardware solution. The bridging of these technologies enhances and facilitates an easy migration path from DES to RSA-based applications.

Secure Enrollment Solutions

Atalla's Card Activation and PIN Selection (CAPS) system and PINS2000 Personal PIN Selector system enable debit and credit card customers to select their own personal identification numbers (PINs). Customers are more likely to use their credit and debit cards with greater frequency when they can select their own PIN.

CAPS is a fast, convenient, and secure way of administering customer-selected PINs in bank branch offices. With CAPS, you can issue a new credit or debit card and show a customer how to use itall within minutes.

PINS2000 allows customers to select PINs conveniently in their homes or workplaces, and gives you a complete turnkey system for administering the PIN selection process.

Point-of-Entry Devices

The Atalla Personal Transaction Machine (APTM) is a secure, customer-activated device that accepts card-based payments at the checkout counter. This compact device is designed with a ATM-like interface, small enough for hand-held use, and occupies minimal space at the checkout counter. The APTM provides a turnkey solution for the popular IBM 4680/83 multilane store system, Fujitsu-ICL electronic cash registers and PS/2 and PC-based cash register systems.

APTM can also be configured to automate customer identification at the bank branch teller window. This solution reduces the time it takes tellers to complete transactions by streamlining the identification process. With APTM, tellers don't have to worry about fraudulent IDs and forged signatures. Customers identify themselves quickly and easily by using their ATM cards and entering their personal identification numbers (PINs) into the APTM as they do at ATMs. The APTM can be complemented with an Atalla AR2000 CheckReader for reading and accepting magnetically encoded checks.

Atalla Challenge Response (ACR) is an economical personal identification device that verifies the identify of any user who attempts to access a computer system cryptographically protected by an Atalla network security processor or module. A hand-held device similar in size to a pocket calculator, the ACR has a keypad and a display. When system access is requested, the user calls the host via a telephone or PC. The user enters his or her unique PIN number selected during the initialization process. The ACR verifies the user's PIN, allowing the transaction to proceed. Next, the host issues a challenge number encrypted under the master file key within the host. A working key generated by the host is stored within the ACR. When the user enters the challenge number into the ACR, it issues a response cryptographically identified within the host. The host compares the response number provided by the ACR with the challenge number encrypted under the master file key. If the numbers match, the user is verified for access.

Cryptographic Security Management Software

Atalla's Cryptographic Security Manager (CSM) software substantially reduces the cost and time of adding cryptographic protection to Tandem NonStop server applications. CSM is the foundation of an integrated end-to-end security architecture that protects critical transactions across financial or informational networks. Used in conjunction with Atalla network security processors and modules, CSM provides basic cryptographic services, including:

- □ Key management
- □ Data encryption and decryption
- □ Message authentication
- □ PIN translation and verification

The Relationship between Atalla and Tandem

Atalla is a division of Tandem Computers. It was acquired in 1987 to help develop a strategy for securing all Tandem on-line transaction processing (OLTP) computer systems. Atalla currently employs approximately 70 people located in the U.S., Canada and Europe.

Support and service are provided by more than 70 Tandem U.S. sales offices and more than 40 Tandem international offices.

Executive Management

Robert Gargus, *President and General Manager,* joined Atalla in March 1993. Bob began his career at Tandem in 1984 as Controller of Manufacturing. He subsequently held the positions of Director of

Materials and Financial Services and Treasurer. He was appointed Vice President and Corporate Controller in September 1987, reporting to Tandem Vice President - Chief Financial Officer David Rynne.

In his position as Corporate Controller, he was responsible for financial planning, management reporting, measurement systems, financial information system, disbursement accounting (payroll, accounts payable, and employee reimbursement), travel, fixed assets and various accounting functions responsible for public reporting.

Prior to joining Tandem Computers, Mr. Gargus spent thirteen years in finance positions at Burroughs Corporation, now Unisys Corporation.

He holds a Masters Degree in Business Administration with a major in Finance from the University of Detroit.

Gary Sabo, *Vice President and General Manager, Internet Business Group (IBG),* joined Atalla in March 1994. Prior to heading the IBG, Gary was Vice President of Product Management and Marketing for AtallaÕs banking and retail products. Formerly the Director of Product Marketing, Client/Server Group for Tandem Computers, Cupertino, California, Gary was responsible for creating and delivering marketing programs related to TandemÕs strategic directions in Open Access, Client/Server, and Applications Development Environment.

Gary also has extensive international experience. He was a founding member of TandemÕs Intercontinental Division and spent 10 years in developing emerging markets in Japan, Asia, Australia, Canada, and Latin America. Gary held various marketing and support management positions including Director of Marketing and Technical Support for the ICON area and General Manager for TandemÕs S.E. Asia sales operations based in Singapore.

Gary joined Tandem in 1976 and held positions in corporate technical education, corporate sales support, and field customer support before moving into marketing and international management.

Gary is a graduate of Purdue University, 1964, B.S. Science, and graduated from the Advanced Management Program, Asia/Pacific Business Studies, at the University of Hawaii, 1988.

Richard D'Angelo, *Vice President, Sales and Marketing, Banking and Retail Business Groups,* joined Atalla in 1996. Prior to joining Atalla, Richard was Vice President of Indirect Channels and Solution Sales for Pyramid Technology Corporation, where he was responsible for partner sales and marketing programs, including the recruitment of VARs, OEMs and ISVs. Richard joined Pyramid in 1994 and held several sales management positions, including the management of international indirect channels and strategic accounts.

Prior to joining Pyramid, Richard held the positions of Sales Director of the Western Region for MasPar Computer Corporation and General Manager for Western Operations for Sequent Computer Systems, Incorporated. Richard also held various sales management positions in his 14 years with the Hewlett Packard Company.

Richard received his BachelorÕs and a MasterÕs degree in Business Administration from Northeastern University.

Dr. Dale Hopkins, *Vice President, Internet Technology,* spent 12 years at IBM in various research and development positions prior to joining Atalla in 1981. While at IBM, Dr. Hopkins worked on the development of advanced electro-optical detection systems, cryptographic techniques used in the

architecture of advanced electronic funds transfer systems and systems architecture for IBM Financial Systems Development.

Since joining Atalla in 1981, Dr. Hopkins has been a significant contributor to the development and success of marketing network interchange security systems to financial institutions.

Dr. Hopkins is a member of the Institute of Electronic and Electrical Engineers (IEEE) Information Theory Group and Sigma Xi, a scientific honors society.

Dr. Hopkins received his B.S. and M.S. Degrees in physics from the University of Louisville and his Ph.D. in electrical engineering from the University of California at Los Angeles. He was a post-doctoral fellow at UCLA and an IBM resident fellow.

Marty Dasher, *Vice President, Alliance Sales & Marketing*. first joined Atalla in 1979 andspent four years building the sales and marketing organization. He returned to Atalla in 1991 and is responsible for establishing third party alliance relationships with software and hardware manufacturers. In addition, Marty has been instrumental in the development and implementation of a new marketing focus at Atalla.

Marty has a proven track record of success for over twenty years in high tech business. He is a graduate of Marquette University in Milwaukee, Wisconsin, where he holds a B.S. in Marketing and Minors in Computer Science and Management.

Thomas Collins, *Vice President of Development,* joined Atalla in April 1995. Prior to joining Atalla, Dr. Collins worked for IBM and Tandem Computers. After 20 years of experience in high technology at IBM, Dr. Collins joined Tandem Computers in Cupertino, CA in March of 1981. He was one of the key individuals in bringing VLSI technology to the Tandem corporation.

Upon joining Tandem, Dr. Collins managed the successful construction and operation of the VLSI Fabrication Facility that included IC wafer fab, packaging, testing, device design and circuit simulation. In 1989, Dr. Collins became Director of Engineering Operations in the Systems Development Division with major responsibilities for product assurance and quality. Dr. Collins spearheaded Tandem' s NSK Quality efforts, resulting in the recent success of ISO 9001 certification.

Dr. Collins holds several patents and has published a number of papers in a variety of technical journals. He was the recipient of IBM's Outstanding Contribution Award and the Third Level Invention Award. In 1984, he was selected for the Tandem Outstanding Performer Award (TOPS) for his efforts in VLSI. Dr. Collins is a Senior Member of the IEEE, editor of the *IEEE Circuits and Devices Magazine*, and a member of Sigma XI Honorary Society.

Dr. Collins received his BSEE from San Jose State University and was awarded its Distinguished Alumni Award in 1995. He received an MSEE from the University of California, Berkeley and a Ph.D. from the University of California, Davis/Livermore Campus as an IBM Resident Graduate Fellow.

Dr. Collins is the Chairman of Tandem's Regulatory Compliance Committee and a member of Tandem's Corporate Practices Committee.

Mark Dentinger, *Controller,* joined Atalla in February of 1994. Prior to joining Atalla, Mark was the Manager of Financial Reporting at Tandem.

Before Tandem, Mark spent ten years with Ernst & Young in the San Francisco Bay Area where he serviced clients in various high-technology fields including the computer manufacturing and software industries.

Mark is a member of the American Institute of Certified Public Accountants. He holds a B.S. degree in Economics from St. Mary's College of California and an M.B.A. in Finance from the University of California at Berkeley.

For more information, contact:

Mark Pickens, Director of Telebusiness (408) 435-5389. Or call 800/523-9981, 408/435-8850.

ActivCard authenticates users across all platforms for all major communications networks including the Internet, public switched networks, cellular, and local and wide area networks.

The Company

Company Overview

> *"Fool-proof, easy-to-use, end-to-end security in a network environment (can) only be provided by security services such as encryption and authentication."*
>
> **- Strategic Networks Consulting, Inc. *The Internetwork Advisor***

ActivCard, Inc. manufactures challenge-response and time-event authentication products for use in standards-based computer security solutions for all major communications networks, especially the Internet, but also including public switched networks, cellular networks, LANs, and WANs. ActivCard works with all major computer and communication terminal devices, including desktop and portable PCs, workstations, t telephones, cellular phones and facsimile machines.

Customers include companies in the aerospace, automotive, health care, technology, manufacturing, financial and telecommunications industries. Products are distributed through original equipment manufacturers (OEMs) and indirect sales channels, including value-added resellers (VARs), system integrators, software developers and distributors. The company maintains a direct sales staff located in offices throughout the Americas, the European arena and Asia.

Home NewsDesk Products Mall Do Business

ActivCard Security

> *" We don't trust anyone on the Internet without strong authentication. (Static) passwords are not good enough. They are too easily guessed or stolen."*
>
> **- Cheswick and Bellovin, Firewalls and Internet Security**

An Extraordinarily High Level of Authentication Security

ActivCard authentication provides an extraordinarily high level of security. The system relies on dynamic passwords generated with DES, a public and widely tested, industry-standard algorithm. The authentication process is initiated by the entry of a PIN which is contained in the token and never transmitted over the computer or communications network, where it can be observed. Network security administrators, not ActivCard, the company, have exclusive control of the secret user keys required by each token. Network administrators download keys into the token and the authentication server. The secret keys are enciphered for secure database storage and cannot be observed or recovered. And the security features of the ActivCard token are stored in the token's random access memory (RAM) and therefore cannot be compromised. A combination of time plus event values to calculate true one-time-use passwords makes ActivCard passwords the most secure passwords on the market.

Full Compliance with International Security Standards

The ActivCard token and related products have been designed and manufactured to meet all relevant international security standards, including those promulgated by ISO and ANSI. For example, to generate its dynamic passwords, the ActivCard token uses the ANSI X3.92 DES algorithm, a public and tested algorithm. The ActivCard Token also complies with the ANSI X9.9 standard for the calculation of dynamic passwords, and with the ANSI X9.17 standard for the management of the secret keys used by the security functions of the ActivCard token.

Home NewsDesk Products Mail Do Business

NetLink Technologies, Inc.

3333 S. Wadsworth Blvd. Suite 200D, Lakewood. CO.
(303) 985-8223 (800) 646-6415 Fax (303) 985-5503

MOTOROLA

E-mail Sales Assistance or call Toll Free 1-800-646-6415 for your Discount Price Quote

Superior Network Authentication Security Simplifiying User Logins

It is now easy to use Network Authentication with a Motorola SecurID Modem providing superior network authentication security while simplifying user login procedures. This multi-function PC Card combines Motorola's high-performance 28.8 modem technology with Security Dynamics' SecurID network authentication. SecurID Modem is compatible with SecurID Access Control Modules, Access Control Encryption (ACE) and ACE/Servers.

Sends and receives data and faxes quickly and accurately - with Motorola's industry-leading 28.8 Kbps (V.34) modem technology.

Features Security Dynamics' two-factor authentication for better network security - network login process combines a user's password or pin number with a randomly-generated access code that changes every 60 seconds.

Connects to leading cellular phones - access important business information whether you're in the office

or on the road-even when phone lines aren't available.

Low power consumption and sleep mode - for extended battery life on mobile computers.

The SecurID Modem PC Card comes complete with full-featured communications software with many advanced features designed to increase productivity.

Frequently Asked Questions

E-mail Sales Assistance or call Toll Free 1-800-646-6415 for your Discount Price Quote

---

SecurID Feature/Benefits:

□ Automatic authentication-the SecurID Modem automatically detects a request for authentication, requests the user's pin number and sends information to the remote host.

□ Functions as a V.34 modem when connected to a host that is not enabled with Security Dynamics' technology.

□ Compatible with Security Dynamics Access Control Modules and ACE/Servers, Apple Remote Access and Shiva™ LAN Rover.

Fax/Modem Feature/Benefits:

□ Intuitive communications software simplifies use of both fax and modem.

□ Maximum 115 Kbps data throughput using compression (V.42bis) at 28.8Kbps (V.34).

□ 14.4 Kbps fax performance.

□ Hardware-based power management.

□ V.42 error correction (LAPM and MNP™ 2-4) ensures the integrity of transferred data.

□ V.42bis and MNP5 data compression.

□ Enhanced Throughput Cellular (ETC) error correction protocol.

□ Extensive AT command set in hardware.

□ **Motorola PC Cards are backed by a five-year limited warranty.**

E-mail Sales Assistance or call Toll Free 1-800-646-6415 for your Discount Price Quote

---

Specifications:

□ FCC Part 15, Class B

□ UL 1950, 1st edition; UL478 5th edition, CSA 22.2 #220; FCC Part 68; CSA 03

Telephony

□ Data Modem:
ITU-T
V.34: 28,800-2400
V.32terbo: 19,200, 16,800 (TCM)

□ CCITT
V.32bis: 14,400, 12,000, 7200 (TCM)
V.32: 9600 (TCM), 4800 (QAM)
V.22bis: 2400 (QAM)
V.22: 1200

□ (DPSK)
V.21: 300 (FSK)
V.23: 600/75, 1200/75 (FSK)
Bell 212A: 1200 (DPSK)
Bell 103: 300 (FSK)

□ Fax Modem:
Compatibility Interface:
EIA-578 (Asynchronous Facsimile Modem Control Standard, Service Class 1)
CCITT
V.17: 14,400, 12,000, 9600, 7200 (TCM)
V.29: 9600 (QAM), 7200 (QAM)
V.27terbo: 4800 (DPSK), 2400 (DPSK)
V.21 Channel 2: 300 (FSK)

Additional Standards

□ PCMCIA Release 2.1 and extensions; Type II

□ Register and architectural compatibility with a 16550 UART that adheres to the I/O and interrupt conventions established under the AT (IBM PC) definitions for COM 1-4

- □ Temperature 32° to 158° Farenheit (0° to 70° Celsius)
- □ Humidity: 10-90 percent noncondensing Connector

- □ Dual RJ-11 Connector (female): enables modem and telephone to be connected to a single phone line

- □ Type II PC Card
- □ Length: 3.37 in/8.56 cm
- □ Width: 2.12 in/5.4 cm
- □ Thickness: 0.19 in/0.5 cm

- □ SecurID modem can be used with most communications programs that support PCMCIA devices, including those running under: Microsoft Windows and DOS, Apple Mac OS and UNIX

- □ 28.8 PCMCIA Type II modem
- □ Dual RJ-11 modem connector
- □ Telephone cable
- □ SecurID Modem User's Guide
- □ Installation diskette (configuration utility software)
- □ Quick Install card

Ordering Information:

E-mail Sales Assistance or call Toll Free 1-800-646-6415 for your Discount Price Quote

PC Card Online Registration

Home Page | Corp. Info | Product Info | Contact Info | What's New

Home Page | Corporate Info | Product Info | Contact Info | What's New

NETLINK TECHNOLOGIES, INC.
3333 S. Wadsworth Blvd.
Suite 200-D

Lakewood, CO 80227
Toll Free 1-800-646-6415 or FAX 303-985-5503
E-mail: nl@interlinkweb.com

Questions, comments or suggestions please E-mail: nl@interlinkweb.com